MRX User Manual

Release 1.13.0

Cybertec Pty Ltd

20 July, 2026

Documentation Control

Document Number: 0013-001-000507

Document Release: 1.13.0

Document Release Date: 20/07/2026

Firmware version: 1.9.10.0

Generation date: 20/07/2026

Release History

V1.3.0 - 12/05/2023 - Updated document formatting.

V1.4.0 - 15/11/2023 - Improvements to document formatting and minor content updates.

V1.5.0 - 25/09/2024 - Updates to several sections to reflect changes in the latest firmware.

V1.6.0 - 12/03/2025 - Updates to several sections to reflect changes in the latest firmware.

V1.7.0 - 01/08/2025 - Updates to access control and security sections.

V1.8.0 - 15/12/2025 - Formatting improvements and updates to reflect changes in the latest firmware.

V1.9.0 - 01/07/2026 - Updates to reflect changes in the latest firmware version.

V1.10.0 - 10/07/2026 - Improvements to AT Command appendix.

V1.11.0 - 15/07/2026 - Corrections and improvements to AT Command appendix.

V1.12.0 - 16/07/2026 - Corrections and improvements to the System chapter.

V1.13.0 - 20/07/2026 - Clean up of the document, fixed references and improvements to the AT Command appendix.

Legal Information

Copyright © 2026 Cybertec Pty Ltd. All rights Reserved.

CONTENTS:

CHAPTER

ONE

INTRODUCTION

This manual describes the functionality and management features of the operating system MRX. The MRX firmware controls the operation of the Cybertec range of modem / routers.

1.1 Document Structure

The first section of the document describes the configuration interface and how to access it. The second section contains specific information for configuring the device.

1.2 Differences between devices running MRX

Not all devices support all features described in this manual. This is usually hardware dependant, for example a 5G/LTE Wireless model may not include an DSL interface, so the DSL chapter will not be relevant.

1.3 Conventions Used

This manual uses the following typographical conventions:

Italic
: Used for emphasising new terms when first introduced.

http://www.cybertec.com.au
: Used to display URLs (Web addresses).

Menu→Submenu
: Used to illustrate menu navigation.

Button
: Used to indicate the name of a button or other GUI element.

`Monospace`
: Used for commands, file names, and other text that should be entered verbatim.

1.3.1 Admonitions

Hint

Indicates a reference to further information. This may include other documents or information available online.

Tip

Indicates a tip or suggestion relating to the occupying text.

Note

Indicates a note relating to the occupying text.

Warning

Indicates a warning or caution relating to the occupying text.

1.4 Manual Updates

Improvements and updates to this manual will be made available on the Cybertec website http://www.cybertec.com.au There you will also find, further product documentation including application notes, user guides, and other support information.

1.5 Default Configuration

Unless otherwise stated the manual assumes the configuration of the unit is in the factory default state. If the modem has been previously configured it may be necessary to perform a configuration reset to return the the configuration to the default state, prior to configuring the device. The procedure to perform a configuration reset is described in the manual for the particular model.

CHAPTER

TWO

ACCESSING THE WEB INTERFACE

This section describes how to connect to the web interface of the unit to be configured. As all configuration is performed via the web interface establishing a connection to the web interface is the first step in configuring the device.

The web interface can be accessed from any interface which supports TCP/IP and provides support for both the HTTP and HTTPS protocols. The description which follows describes accessing the web interface via the Ethernet interface. It is also possible to access the web interface via the wireless interface however to do this the firewall will need to be configured to allow incoming connections.

Note

For best results it is recommend that a modern web browser be used with JavaScript enabled. The web interface makes use of JavaScript although it is possible to use a browser with JavaScript disabled not all functionality will be supported.

2.1 Computer Settings

In order to view the web pages a computer with a fixed IP address, on the same sub-net as the unit to be configured, will need to be connected to one of the LAN ports.

- **The default IP settings of the unit are:**
  - IP Address: 10.10.10.10
  - Netmask: 255.255.255.0
- **The recommended IP settings for the PC used to configure the unit are:**
  - IP Address: 10.10.10.20
  - Netmask: 255.255.255.0
  - Default Gateway: 10.10.10.10
  - Primary DNS: 10.10.10.10

Warning

Although it is possible to connect the unit to be configured directly to a Local Area Network (LAN) it is recommend that the network configuration as described in this section be performed prior to doing so.

2.2 Windows PC Network Settings

The following describes how to configure the network settings of a Windows XP PC with the IP settings listed above.

Warning

This procedure will change the network settings of the Windows PC, if the PC is connected to a network the connection should be removed before performing the changes. To restore the network settings of the PC record the current settings TCP-Settings in the following procedure, then once configuration of the unit has been completed use the recorded values to restore the Windows PC network settings.

1. Open the Control Panel by selecting *Start* → *Control Panel*

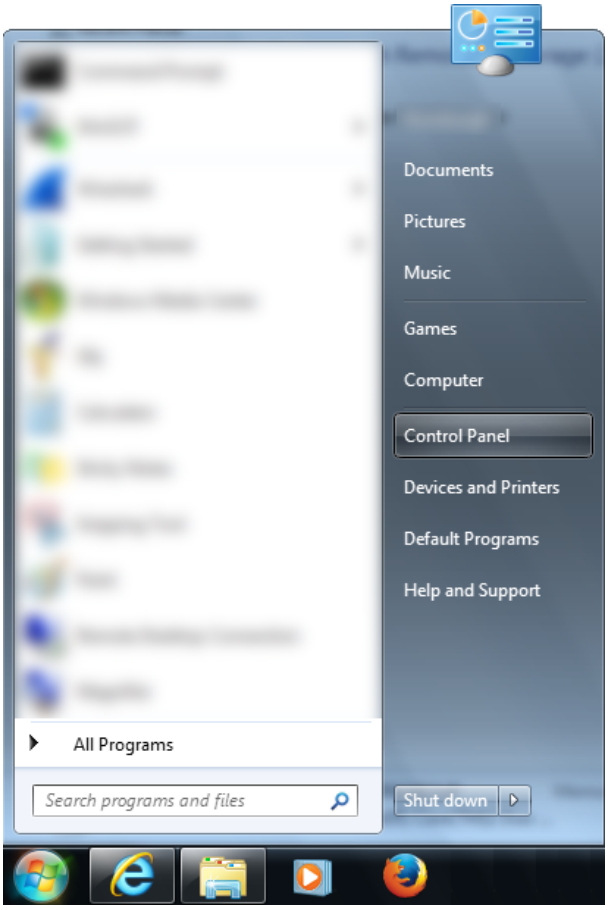


Fig. 2.1: Select Control Panel from the Start menu.

2. The Control Panel will be displayed.

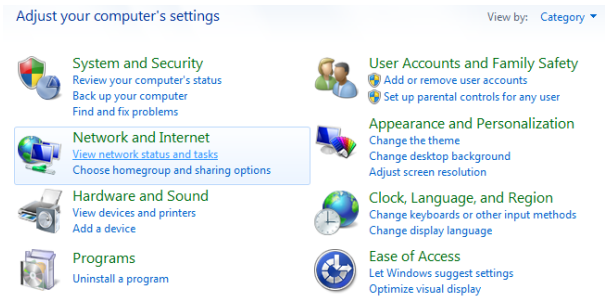


Fig. 2.2: The Control Panel with Network and Internet highlighted.

3. Under the section titled Network and Internet click the link View network status and tasks.
4. The Network Sharing window will be displayed. Click the link Local Area Connection which is in the section titled View your active networks.

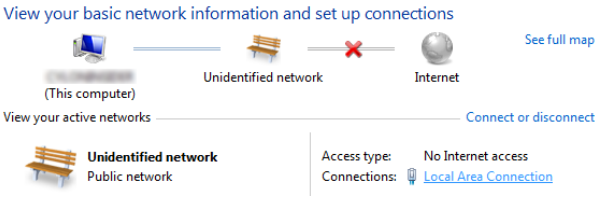


Fig. 2.3: Network sharing options.

5. The Local Area Connection Status dialogue box will be displayed, as shown on the left of Fig. 2.4, click the Properties button.

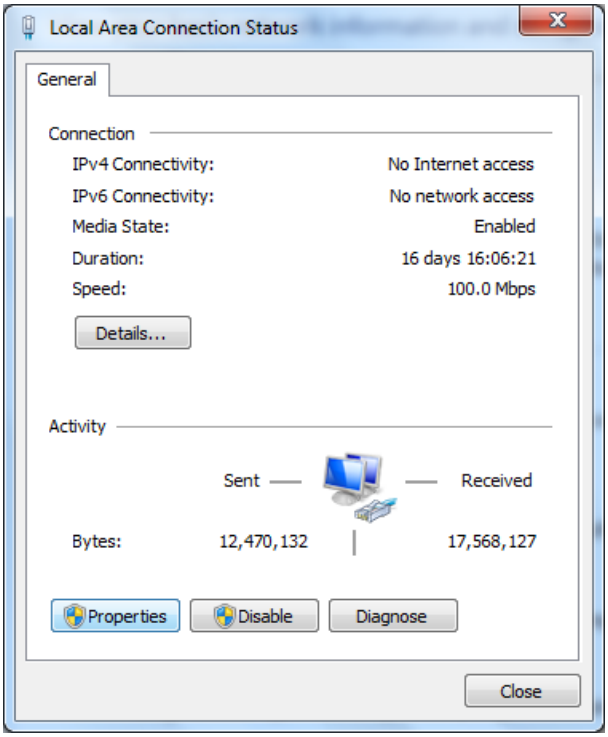


Fig. 2.4: Local Area Connection Status and Properties dialogue boxes.

6. The Local Area Connection Properties dialogue box, as shown on the right of Fig. 2.5, will be displayed. Click on Internet Protocol (TCP/IP) to highlight it and then click the Properties button.
7. The Internet Protocol (TCP/IP) Properties dialogue box, change the settings to match those shown in Fig. 2.6, and then click "OK"

Note

If a web browser was open prior to making the network changes, then it will need to closed and re-started before attempting to connect.

2.3 Connecting to the Web Server

- Open a web browser on the PC and browse to the default IP address for the unit as shown:
- A page similar to Fig. 2.8 will be displayed. An administrator password for the user 'admin' will need to be entered. The password set will be required for subsequent logins.
- Click the Set Password button to set the admin password and login.

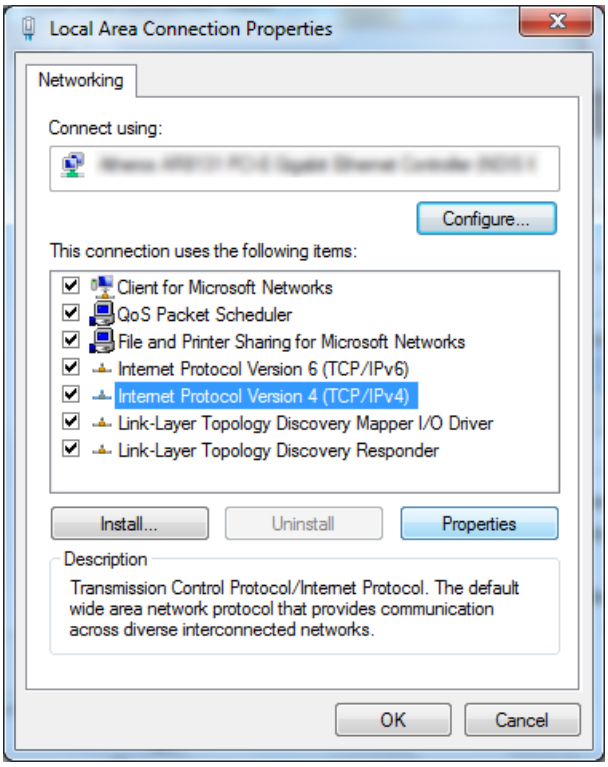


Fig. 2.5: Local Area Connection Status and Properties dialogue boxes.

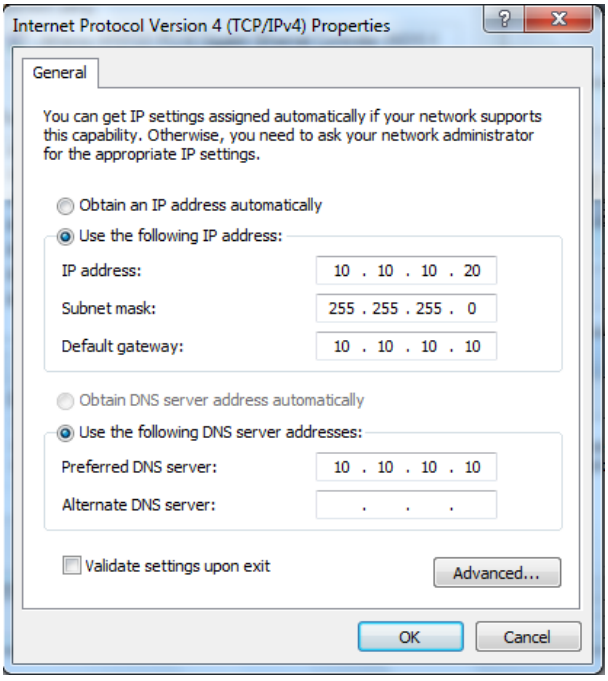


Fig. 2.6: TCP/IP Properties dialogue box showing the recommended IP settings.

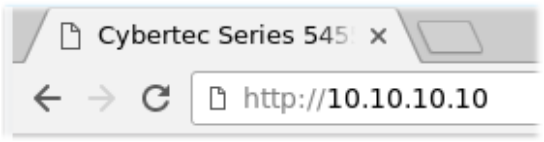


Fig. 2.7: Web Address entry.

Fig. 2.8: Set Administrator Password shown on first boot.

Note

If the box fails to display, re-check the cable connections to the unit and the IP address settings of the PC.

- The standard login is shown in *Web login box completed.*, if a password has already been set this is the prompt that will appear. To continue the admin password will need to be entered.

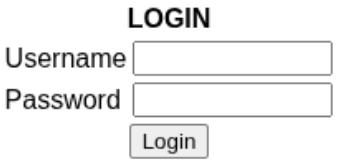


Fig. 2.9: Web login box completed.

- Click the Login button to login.
- The Status summary page will be displayed, it will be similar to Fig. 2.10

Note

As the unit has not yet been configured it is likely that some faults will be indicated.

Note

A warning is shown indicating the default password is set. The password should be changed before continuing with further configuration.

Details on how to change the password are in section *Editing users and passwords*

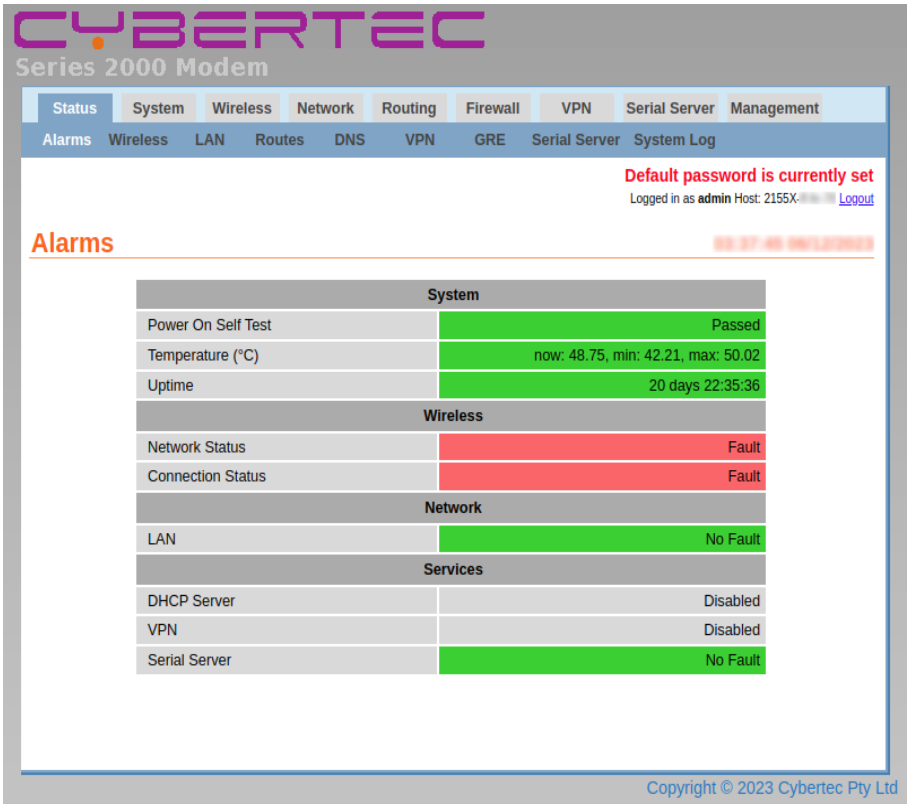


Fig. 2.10: Status summary page.

CHAPTER

THREE

WEB PAGE LAYOUT

This chapter describes the web page layout and menu structure. The pages are arranged in functional groups accessible via the main menu. For each main menu a number of sub-menu pages provide access to specific information and setting. When a main menu item is select the first sub-menu page is automatically displayed.

This section does not described how to connect to the web interface of the device. For information on connecting to the web server of the device refer to the section *Accessing the Web Interface*.

3.1 Page Layout

To illustrate the page layout the Status web page is shown in Fig. 3.1, this is first page to be displayed when a connection to the web server is established. At the top of the page, under the Cybertec logo is the menu which consists of two rows of tabs. The top row is the main menu, the sub-menu tab row is directly under the main menu. The main menu tabs are used to select a group of related pages and the sub-menu is used to select a page within that group. When a main menu tab is selected the sub-menu option tabs will change allowing individual pages within the group to be selected.

Below the menu is the page title. The title indicates the selected page. Below the title is the page body. This section will contain information and/or configuration settings for the selected function.

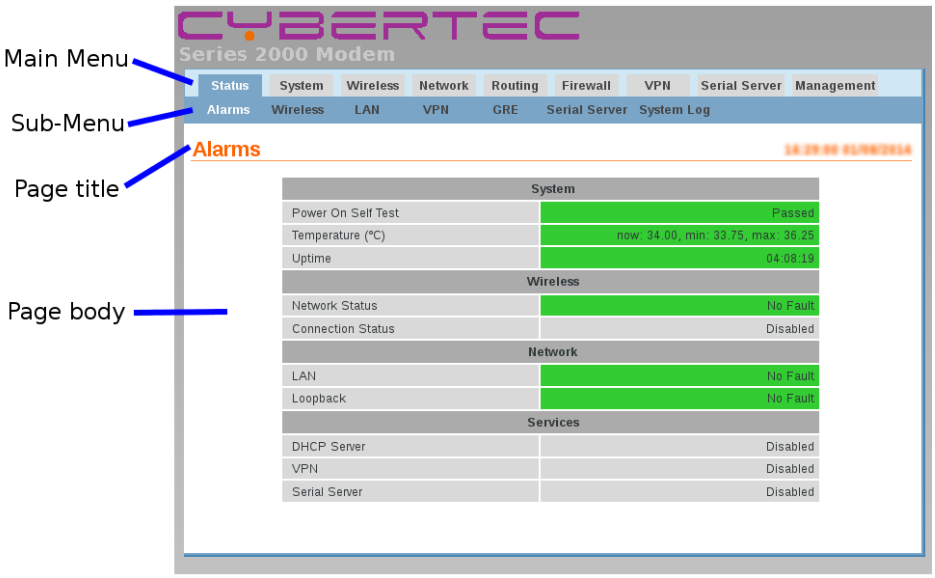


Fig. 3.1: Web page structure.

Note

When a menu item is referenced in the manual it is in the form *Menu* → *Sub-Menu*

For example *Status* → *Alarms* would refer to the Main Menu Status / Sub-Menu Alarms page as shown in Fig. 3.1.

3.2 Menu Structure

The section provides a brief description for each of the main menu tabs and for each sub-menu tab.

Note

Not all items listed will be available on all models.

For example GPIO will only be displayed for models which have GPIO hardware.

3.2.1 Status

The Status tab is used to report the current operating status of the unit.

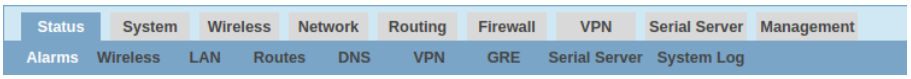


Fig. 3.2: Status menu - Wireless version.

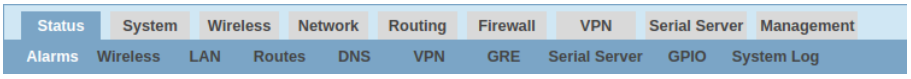


Fig. 3.3: Status menu - Wireless with GPIO.

Fig. 3.4: Status menu - DSL version.

Alarms
: A summary of the alarm status.

Wireless
: Reports the status of the wireless connection.

LAN
: Information on the LAN settings

VPN
: Reports the status of any active VPNs

GRE
: Reports the status of any active GRE tunnels

Serial Server
: Provides an overview of the Serial Server and serial ports.

GPIO
: Reports state of I/O and sets states of outputs.

SystemLog
: A log of the system messages.

3.2.2 System

The System tab provides system level information and configuration settings.

Fig. 3.5: System menu - Wireless.

Fig. 3.6: System menu - Wireless with GPIO.

Fig. 3.7: System menu - DSL version.

Administration
: Set host-name, configure the NTP connection, change passwords, set timed re-boot and reboot the modem.

Backup & Upgrade
: Backup and restore the configuration, upgrade the firmware.

Information
: Reports model number, serial number, firmware versions, MAC address and wireless IMEI & IMSI.

Syslog
: Remote syslog settings.

Power
: Configure the power controller for automatic power shut-down and start-up.

GPIO
: Configure the digital I/O.

Location
: GPS configuration.

Support
: Generate a Technical Support file for reporting purposes.

Certificates
: Certificate Management

3.2.3 Wireless

The Wireless tab provides access to the wireless settings.

Network
: Operating mode, frequency band selection and SIM card PIN settings.

Network Selection
: Network operation selection.

Packet Mode
: Profile management and selection, connection state selection.

Connection Management
: Connection establishment and maintenance options.

Fig. 3.8: Wireless menu.

SMS
SMS triggers and access control.

3.2.4 DSL

The DSL tab provides access DSL settings, this includes the VDSL and ADSL settings and the options for setting the operating mode.

Fig. 3.9: DSL menu.

Network
The line and interface general settings.

VDSL
The settings for VDSL operation.

ADSL
The settings for ADSL operation.

Connection Management
The connection management settings.

3.2.5 Network

The Network tab is used to access the Local Area Network (LAN), Dynamic Host Configuration Protocol (DHCP) and DNS settings.

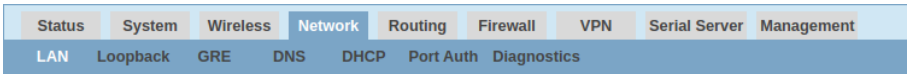


Fig. 3.10: Network menu

LAN
LAN and DHCP settings.

Loopback
Loopback interface settings.

GRE
Generic Routing Protocol settings.

DNS
Manual and Dynamic DNS settings.

DHCP
Manage and configure the DHCP Server.

Port Auth
Ethernet Port Authentication configuration.

Diagnostics
Verify network connectivity with Ping and Traceroute.

3.2.6 Routing

Routing support includes static and dynamic routing as well as policy and Quality of Service (QoS) based routing. Routing options are accessed via the Routing tab.

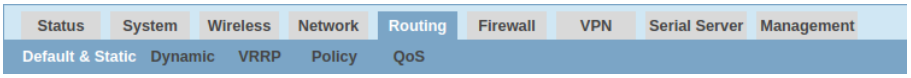


Fig. 3.11: Routing menu

Default & Static
Define the default route and static routes.

Dynamic
Dynamic routing options.

VRRP
Configure the Virtual Routing Redundancy Protocol.

Policy
Define policy based routes.

QoS
Quality of Service (QoS) options and define QoS routes.

3.2.7 Firewall

The Firewall tab allows configuration of the firewall settings which include the definition of port forwards and packet filters.

Fig. 3.12: Firewall menu

Setup
Enable NAPT, stateful packet inspection and connection tracking options.

Access Control
Define which modem services can be accessed from the wireless interface and VPN tunnels.

DoS Filters
Define with Denial of Service filters are enabled.

Custom Filters
Define and edit custom packet filters.

Port Forwards
Define and edit port forwards.

Custom NAT
Define and edit custom Network Address Translation rules.

MAC Filters
LAN MAC Address filtering options.

3.2.8 VPN

The VPN tab provides access to the configuration for the SSL, IPsec, PPTP and L2TP VPNs.

IPsec VPN
Enable and configure IPsec VPN tunnels.

SSL VPN
Enable and configure SSL based VPN (OpenVPN).

Fig. 3.13: VPN menu

PPTP & L2TP
Enable and configure PPTP and L2TP VPN tunnels.

Certificate
VPN certificate management.

3.2.9 Serial Server

The Serial Server tab is used to access the configuration options for the serial server and each of the available serial ports.

Fig. 3.14: Serial Server menu

Port Setup
Configure the serial server port function and configuration options for each of the available serial ports.

Phone Book
Modem dial string phone book management.

3.2.10 Management

The Management tab provides access to the management settings.

Fig. 3.15: Management menu

Events
Configure the actions taken when an event occurs.

SNMP
Configure SNMP parameters.

DNP3
Configure the internal DNP3 outstation.

SMS
SMS control and management.

Email
Email server configuration.

LLDP
Enable or disable Link Layer Discovery Protocol and SNMP reporting.

CLI
Enable or disable SSH and Telnet for Command Line Interface access.

3.3 Symbols

The following symbols are used on the web pages:

	Edit Icon. Click this icon to edit the indicated setting.
	Delete Icon. Click this icon to delete a setting.
OK	OK Button. Click this button to accept a change.
Update	Update Button. Click this button to save changes.
Reset	Reset Button. Click this button to reset the values on the page to the values prior to editing.
Choose file	Choose File Button. Click to choose a file from the local operating system.
Upload	Upload Button. Click this button to upload a file to the unit.
Next	Next Button. Click this button to move to the next page in a multiple page configuration.
Back	Back Button. Click this button to move back a page in a multiple page configuration.

CHAPTER

FOUR

STATUS

The Status pages provide information on the operating state of the unit. These pages will assist in ensuring the unit is operating correctly and if it is not working correctly provide assistance in diagnosing the problem.

Note

The status pages do not refresh automatically. In order to see the current status of a displayed value it may be necessary to refresh the page. This is especially the case for a value which is changing, this could be the case at any time but in particular at start up.

To access the status pages click the *Status* tab on the main menu. A page similar to the one shown in Fig. 4.1 will be displayed.

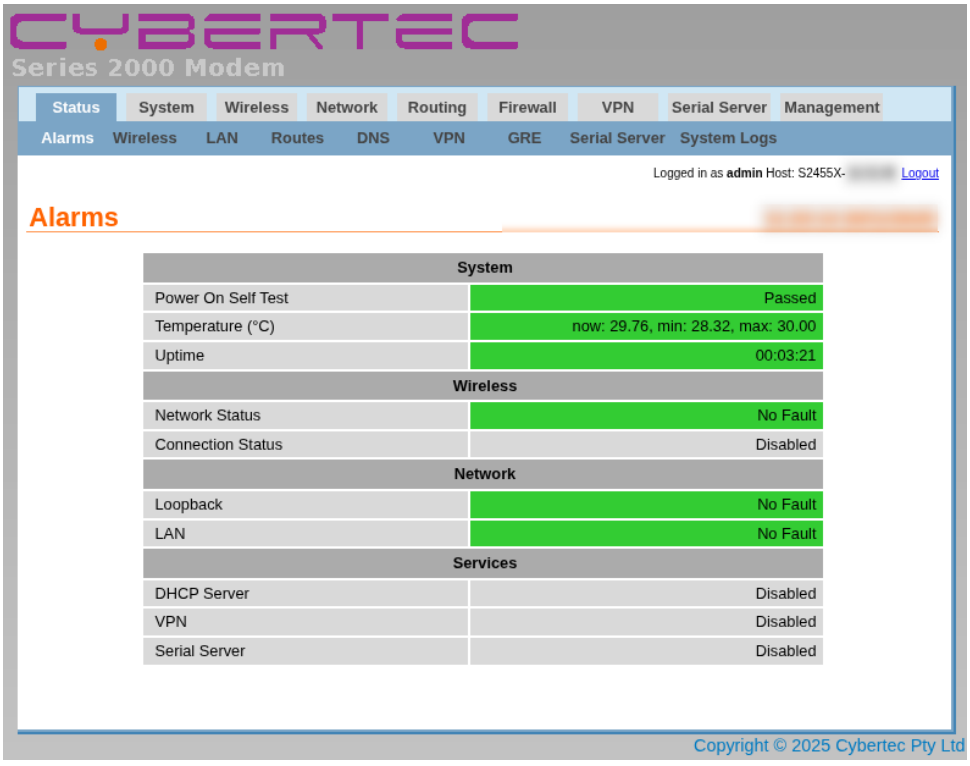


Fig. 4.1: Main status page.

4.1 Alarms

The Status Alarms page is the first page displayed by default page once connected to the device, it can also be selected at any time by clicking *Status→Alarms*.

This page provides a summary of the state of the operating services. A service which is operating correctly will be highlighted green, a service with any error will be highlighted red, services not enabled will be shown with a grey background.

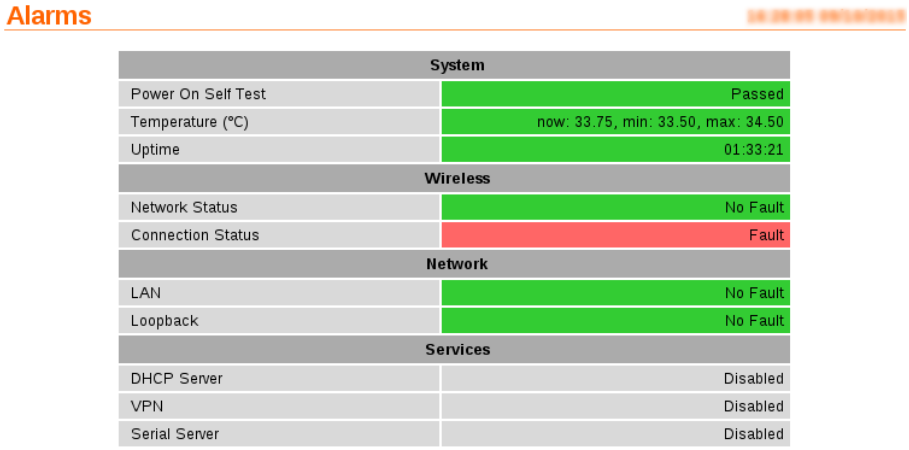


Fig. 4.2: Alarms status page for a Wireless unit, showing Wireless connection status

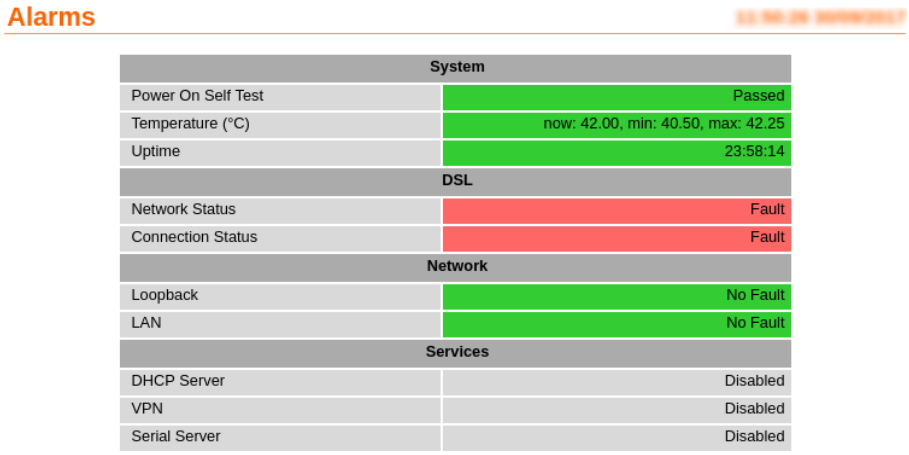


Fig. 4.3: Alarms status page for an DSL unit, showing a connection status fault.

The page is divided into sections representing the status of system level services, the Wireless or DSL interface, LAN interfaces and other services. If a fault is indicated further information can be obtained from the corresponding status page.

For example in Fig. 4.2 a fault is indicated for Connection Status in the Wireless section, further information on the fault can be obtained by selecting the *Status→Wireless* page. Details are described in the sections *Wireless Alarms* and *Wireless Interface Status*.

Similarly Fig. 4.3 shows a fault as reported on a DSL model. Further information on the fault can be obtained by selecting the *Status→DSL* page. Details are described in the sections *DSL Alarms* and *DSL Interface Status*.

4.1.1 System Alarms

Power On Self Test

Indicates the result of the self testing done during the boot sequence. An error would usually indicate a hardware fault and the unit should be returned for service.

Temperature
Indicates the current, minimum and maximum operating temperatures.

Uptime
Indicates the current running time.

4.1.2 Wireless Alarms

Network Status
Indicates the current wireless network connection status. This indicates if the unit has established a connection to the network.

Connection Status
Indicates the current wireless packet or circuit switched data (CSD) connection status.

Further information on the Wireless interface status can be obtained from the *Status→Wireless* page described in *Wireless Interface Status*.

4.1.3 DSL Alarms

Network Status
Indicates the current line connection status. This indicates if the unit has established a connection to the DSLAM.

Connection Status
Indicates the current packet connection status.

Further information can be obtained from the *Status→DSL* page.

4.1.4 Network Alarms

LAN
Indicates the status of the Local Area Network (LAN).

LAN2
Indicates the status of the LAN2 port.

> **Note**
> Only shown if the Independent LAN ports has been enabled and the LAN2 port has been enabled and configured.

Loopback
Indicates the status of the Loopback interface.

> **Note**
> Only shown if the loopback interface is enabled and configured.

Further information on the status of the LAN interfaces can be obtained from the *Status→LAN* page, refer to the section *Local Area Network (LAN)*

4.1.5 Service Alarms

DHCP Server
Indicates the status of the Dynamic Host Configuration Protocol (DHCP) server. Further information on DHCP status can be found on the *Status→LAN* page.

VPN
Indicates the status of any Virtual Private Networks. Further information on the VPN status can be found on the *Status→VPN* page.

Serial Server
Indicates the status of the Serial Server. Further information on Serial Server can be obtained from the *Status→Serial Server* page.

4.2 Wireless Interface Status

The Wireless status page (*Status→Wireless*) provides details of the current operating state of the wireless interface.

The page displayed will depend on the wireless operating mode, Fig. 4.4 shows the page for packet mode, which is supported in all wireless units. While Fig. 4.5, in the next section, shows the page for Circuit Switched Data (CSD) mode which is only supported on some models.

For information on the different wireless operating modes refer to the *Wireless* chapter.

Wireless

Network Status	
Interface	Down
Active SIM	SIM 1
SIM Card	No SIM present
Network Registration	No
Roaming	No
Signal Strength (RSSI)	Unknown
Provider	(Location: / Cell ID:)
Connection Status	
Status	Down
Current Session Time	
Total Session Time	00:00:00
IP Address	0.0.0.0
Session Statistics	
Packets Received	0
Bytes Received	0 B
Packets Transmitted	0
Bytes Transmitted	0 B
Connection Maintenance	
Outstanding Request	No
Interface Restarts	0
Active Poll	disabled

Fig. 4.4: Wireless status page for packet mode.

4.2.1 Network Status (Packet Mode)

The network status section is common for both modes of wireless operation.

Interface
Indicates the state of the wireless interface. The indication will be:

Up
if the wireless interface has established a network connection.

Down
if the wireless interface has not established a network connection.

Active SIM
Reports the current active SIM. The active SIM is only shown for models which support multiple SIM cards and reports SIM 1 or SIM 2.

SIM Card
Reports the state of the SIM.

The indication will be:

OK
If the SIM has been detected and is working correctly.

Error
If the SIM has not been detected or is faulty.

Network Registration
Indicates the network registration state.

Roaming
Indicates if the roaming has been been enabled.

For details on roaming refer to the *Wireless* chapter.

Signal Strength (RSSI)
Provides an indication of the received RF signal Level or Received Signal Strength Indication (RSSI). The RSSI is reported as a value up to 31, the higher the value the greater the received signal level. The actual received level is also indicated as a value in dBm.

Signal Strength (RSRP)
Provides the value of the Reference Signal Received Power (RSRP). This is the measured power of the LTE reference signals spread across the spectrum. The value for RSRP is reports as a value out of 97 with the larger number the higher the signal strength. It is also reported in dBm, which is always negative, and the higher the value in dBm (closer to 0dBm) the greater the signal strength.

Signal Quality (RSRQ)
Provides a value for the Reference Signal Received Quality (RSRQ), which is the ratio of the carrier power to the interference power. This is the signal to noise ratio measured using a standard signal.

The signal quality provides a good indication as to the performance and stability of the wireless connection. A connection with a high RSRQ should be reliable, even if the RSRP is low.

Frequency Band
Reports the currently selected frequency and Radio Access Technology (RAT).

Provider
Indicates the network service provider name and service, the location ID and the cell ID.

4.2.2 Connection Status (Packet Mode)

Status
The packet connection status. The indication will be:

Up
if the wireless packet connection has been established.

Down
if the wireless packet connection has not been established.

Current Session Time
Time the current packet session has been active.

Total Session Time
The total packet session time since boot.

IP Address
The wireless IP address

4.2.3 Session Statistics (Packet Mode)

This section shows the number of data packets and bytes received and transmitted for the session.

Packets Received
The total number of packets received.

Bytes Received
The total number of bytes received.

Packets Transmitted
The total number of packets transmitted.

Bytes Transmitted
The total number of bytes transmitted.

4.2.4 Connection Maintenance (Packet Mode)

This section indicates the status of connection Maintenance. For details on the configuring connection Maintenance for the wireless interface refer to *Connection Maintenance*.

Outstanding Request
Indicates if a poll request is outstanding. Will report:

No
if all polls have received a response.

Yes
if a poll has been sent and a response has not been received.

Interface Restarts
Indicates the number of times connection management has re-started the wireless interface.

Active Poll
Indicates the active polling type.

disabled
Polling is disabled.

ICMP to <IP Address>
The poll type is ICMP (Ping) to the indicated IP address

TCP to <IP Address>
The poll type is TCP socket to the indicated IP address.

4.2.5 Remote poll

This section will provide indication of the remote poll session statistics. There will be a separate section for each poll configured. For a primary only configuration 1 section will be shown, if a backup poll is configured then 2 sections will be shown.

The remote poll heading will be in the form:

Remote poll: <type> to <IP address>
where:

ICMP to <IP Address>
The poll type is ICMP (Ping) to the indicated IP address

TCP to <IP Address>
The poll type is TCP socket to the indicated IP address.

Reported values:

Data Sent
Indicates the number of polls sent.

Data Received
Indicates the number of polls received.

4.2.6 Connection Status (CSD Mode)

> **Warning**
>
> CSD mode is generally no longer supported by network operators and the functionality will be removed in a future firmware version.

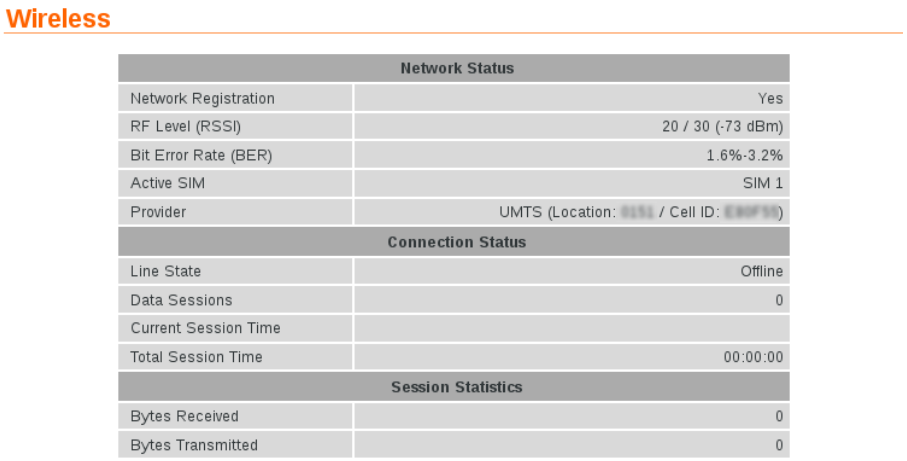


Fig. 4.5: Wireless status page for Circuit Switched Data (CSD) mode.

Line State
The current status of the connection either offline or connected.

Last Dial Result
The result of the last dial attempt.

Data Sessions
The number of successful connections.

Current Session Time
Time the current connection has been active.

Total Session Time
The total time of all connections since boot.

4.2.7 Session Statistics (CSD Mode)

This section shows the number of data packets and bytes received and transmitted for the session.

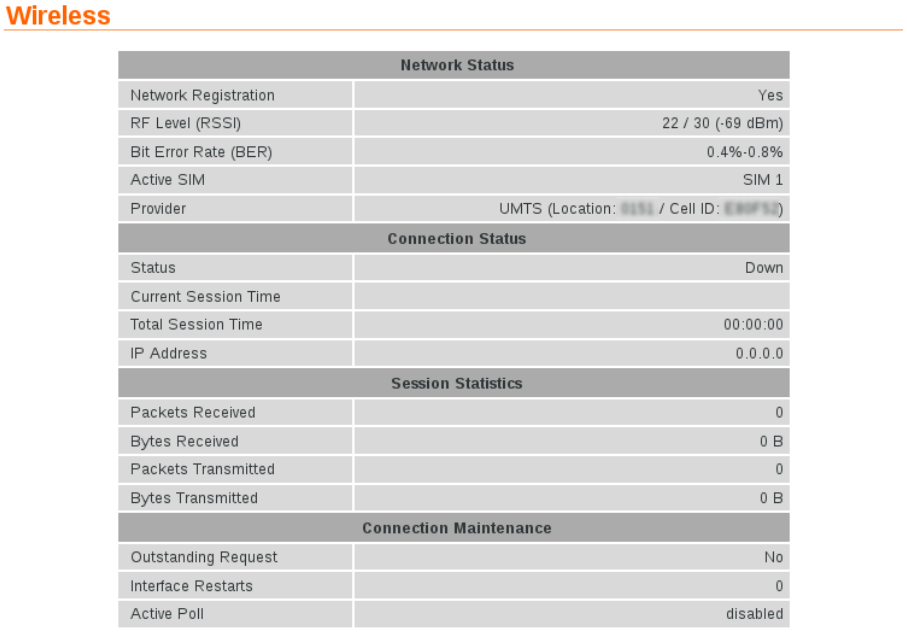
Bytes Received
The total number of bytes received.

Bytes Transmitted
The total number of bytes transmitted.

4.2.8 Connection Status Fault

Continuing the fault example from the *Alarms* section, Fig. 4.6 shows a Connection Status error for a packet mode connection. The error is due a configuration error, indicating that the wireless packet mode settings need to be checked.

For details on configuring the wireless interface refer to the *Wireless* chapter.



Wireless

Network Status	
Network Registration	Yes
RF Level (RSSI)	22 / 30 (-69 dBm)
Bit Error Rate (BER)	0.4%-0.8%
Active SIM	SIM 1
Provider	UMTS (Location: [illegible] / Cell ID: [illegible])
Connection Status	
Status	Down
Current Session Time	
Total Session Time	00:00:00
IP Address	0.0.0.0
Session Statistics	
Packets Received	0
Bytes Received	0 B
Packets Transmitted	0
Bytes Transmitted	0 B
Connection Maintenance	
Outstanding Request	No
Interface Restarts	0
Active Poll	disabled

Fig. 4.6: Wireless status page for packet mode displaying a connection error.

4.3 DSL Interface Status

The DSL status page can be accessed by selecting *Status->DSL* provides details of the current operating state of the DSL interface. A page similar to that shown is Fig. 4.7 will be displayed. For information on configuring the DSL interface refer to the *DSL* chapter.

4.3.1 Network Status

The section provides information on the status of the DSL line connection.

Line Status
Indicates the line connection state. When a connection has been established with a DSLAM this will be indicated with Up.

Mode
Indicates the connection type. For example ADSL, ADSL2+, VDSL it will also indicate the ANNEX and Line profile of the connection.

Framing
The framing type of the connection.

Download Sync (Kbps)
Indicates the download sync speed in kilobits per second (Kbps).

Upload Sync (Kbps)
Indicates the upload sync speed in kilobits per second (Kbps).

4.3.2 Connection Status

The connection status provides details of any packet connections.

Status
The packet connection status. The indication will be:

Up
if the interface is connected; or

Down
if the interface is not connected.

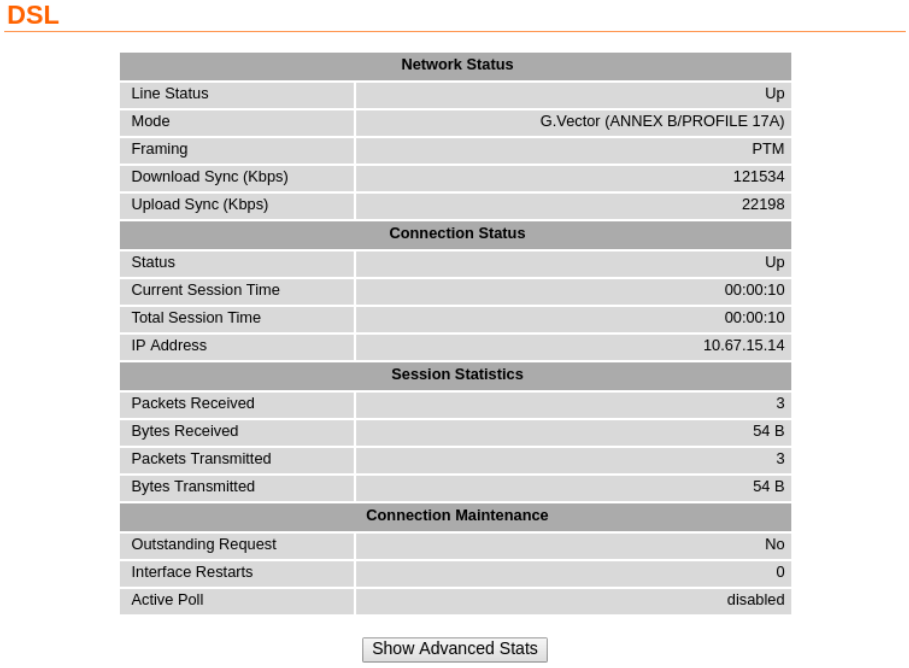


Fig. 4.7: DSL status page.

Current Session Time
The time is since the connection was established.

IP Address
The IP address provided for the connection.

MTU
Reports the Maximum Transmission Unit (MTU) for the interface.

4.3.3 Session Statistics

This section shows the number of data packets and bytes received and transmitted for the session.

Packets Received
The total number of packets received.

Bytes Received
The total number of bytes received.

Packets Transmitted
The total number of packets transmitted.

Bytes Transmitted
The total number of bytes transmitted.

4.3.4 Connection Management

This section indicates the status of connection management. For details on the configuring connection management for the DSL interface refer to Section *Network Configuration* in the *DSL*.

Outstanding Request
Indicates if a poll request is outstanding. Will report:

No
if all polls have received a response.

Yes
if a poll has been sent and a response has not been received.

Interface Restarts
Indicates the number of times connection management has re-started the wireless interface.

Active Poll
Indicates the active polling type.

disabled
Polling is disabled.

ICMP to <IP Address>
The poll type is ICMP (Ping) to the indicated IP address

TCP to <IP Address>
The poll type is TCP socket to the indicated IP address.

4.3.5 Remote poll

This section will provide indication of the remote poll session statistics. There will be a separate section for each poll configured. For a primary only configuration 1 section will be shown, if a backup poll is configured then 2 sections will be shown.

The remote poll heading will be in the form:

Remote poll: <type> to <IP address>
where:

ICMP to <IP Address>
The poll type is ICMP (Ping) to the indicated IP address

TCP to <IP Address>
The poll type is TCP socket to the indicated IP address.

Reported values:

Data Sent
Indicates the number of polls sent.

Data Received
Indicates the number of polls received.

4.3.6 Advanced Connection Statistics

To access the advanced DSL connection statistics click the Show Advanced Status button. The page has 2 sections, the first is the line statistics as shown in Fig. 4.8, and described in the section *Line Status*, The second table contains the Signal Status statistics, Framing details and counters for both upstream and downstream, as shown in Fig. 4.9 and described in the section *Advanced Statistics*.

4.3.7 Line Status

This section provides details of the line level connection.

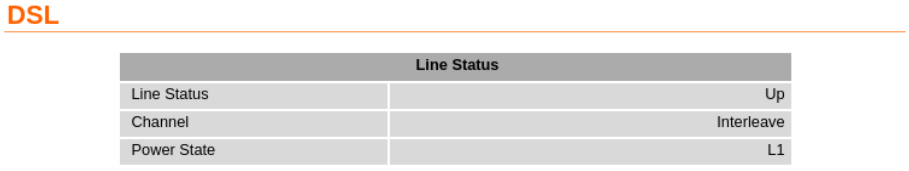


Fig. 4.8: DSL Line Status section of the Advanced Statistics page.

Line Status
The current status of the line.

Channel
The channel type

Power State
The power state.

4.3.8 Advanced Statistics

This section, shown in Fig. 4.9, provides detailed statistical information for the downlink and uplink data. It is divided in 3 sections each of which is described below:

Advanced Statistics		
	Down	Up
Signal Status		
Trellis	On	On
SNR (dB)	0	0
SNR Margin (dB)	142.0	266.0
Line Attn (dB)	24.0	25.0
Signal Attn (dB)	1023.0	1023.0
Pwr (dBm)	98.0	5.0
Sync (Kbps)	121534	22198
Max Sync (Kbps)	121534	62153
PTM Framing		
Bytes	2902	2216
Frames	44	35
OOS	0	0
Errors	0	0
Discard Packets	0	0
Discard Packets	0	
Counters		
Super Frames	3671	3670
Super Frame Errors	0	0
RS Words	81063	0
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	245	0
Total Cells	48375491	8839581
Data Cells	12561	66
Dropped Cells	245	
Total ES	0	0
Total SES	0	0
Total UAS	133	133

Fig. 4.9: DSL Advanced Statistics.

Signal Status

This section provides details of downlink and uplink data lines.

SNR (dB)
The Signal to Noise Ratio for the line.

SNR Margin (dB)
The noise margin above the minimum required for the indicated sync rate.

Line Attn (dB)
The attenuation of the line.

Signal Attn (dB)
The signal attenuation.

Pwr (dBm)
The receive (downlink) or transmit (uplink) power level.

Sync (kbps)
The current data rate at which the connection is synchronised, reported in kilobits per second.

Max (kbps)
The maximum theoretical data rate calculated for the line, reported in kilobits per second.

PTM Framing

This section provides details of the Pulse-Time Modulation (PTM) Framing.

Bytes
The number of bytes sent or received

Frames
The number of frames sent or received.

OOS
Out Of Sync.

Errors
The number of errored frames.

Discard Packets
The number of discarded packets due to error.

Counters

Error counters.

Super Frames
Traditionally, a superfame consists of 24 frames contiguously transmitted together. In ADSL, a superframe consists of 68 adsl frames plus a synchronisation frame. The ADSL modem generates 4000 frames per second. The global duration of an ADSL superframe is 17ms.

Super Frame Errors
Count of the Super Frames received which had an error. This is similar to CRC error.

RS Words
Count of the total number of Reed-Solomon code words transmitted/received.

RS Correctable Errors
The number of Reed-Solomon code words with correctable errors. Reed-Soloman is a method of Forward Error Correction and therefore a count of data successfully recovered. See FEC.

RS Uncorrectable Errors
The number of Reed-Solomon code words that had uncorrectable errors. Reed-Soloman is a method of Forward Error Correction. Uncorrectable Errors are those that are too severe to be corrected by FEC.

HEC Errors
Count of Header Error Check/Correction (HEC) Errors. HEC is a type of CRC error check which has been performed on the header of an ATM cell, but 1 bit errors can be corrected. This count is usually where HECs have been uncorrected and have been discarded. If these errors are too high within a short period of time it will slow throughput and could even lead to connection instability. See Out Of Cell Delineation.

Total Cells
The total number of ATM cells.

Data Cells
The total number of ATM cells containing data.

Dropped Cells
The total number of ATM cells dropped due to error.

Total ES
The number of errored seconds. A one second period of time in which either one or more coding violations occurred OR at least one Loss of Signal events occurred.

> **Note**
>
> It is not unusual to see an occasional Errored Second (ES).

Total SES
The number of Severely Errored Seconds.

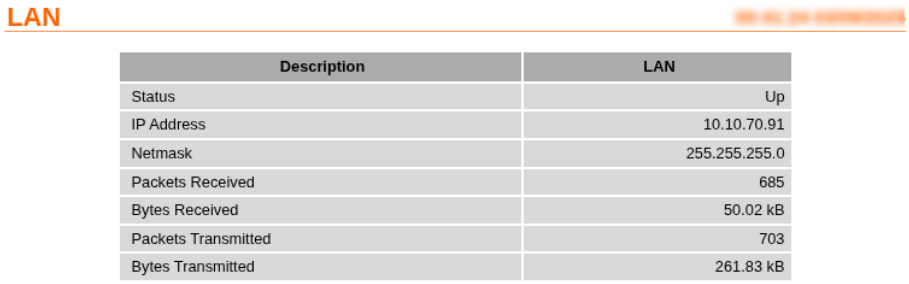
A Severely Errored Second is a one second period which contains 30% or more errored blocks OR several other events such as one or more Out Of Frame (OOF) errors.

Total UAS
Total Unavailable seconds.

Ten consecutive Severely Errored Seconds (SES) will trigger an UAS event, and will remove the path from use. The path will become usable again after 10 consecutive seconds with no SES.

4.4 Local Area Network (LAN)

The Local Area Network (LAN) status page *Status→LAN* provides details of the current operating state of the LAN or Ethernet interfaces. A second section displaying DHCP lease information will be shown if the DHCP server has been enabled. For LAN settings refer to the *Network* chapter.

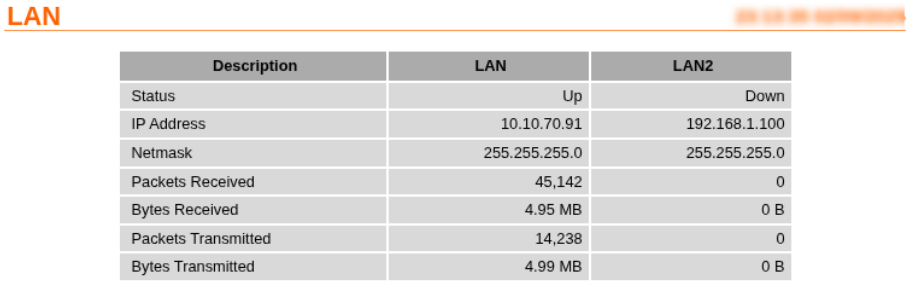


Description	LAN
Status	Up
IP Address	10.10.70.91
Netmask	255.255.255.0
Packets Received	685
Bytes Received	50.02 kB
Packets Transmitted	703
Bytes Transmitted	261.83 kB

Fig. 4.10: LAN Status page.

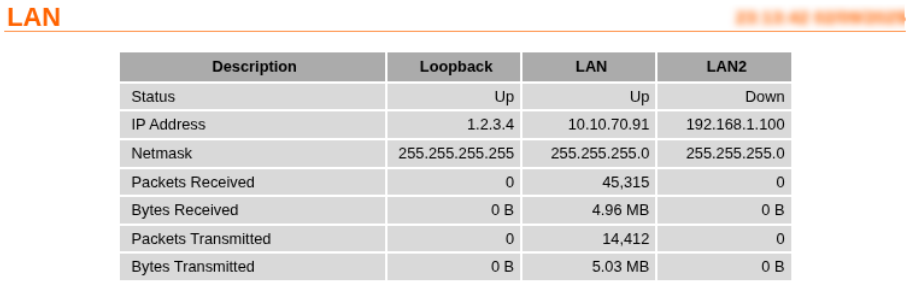
The interfaces listed in the table will depend on the configuration of network interfaces. At a minimum the LAN interface will be listed, as shown in Fig. 4.10.

If the setting “Independent LAN ports” is checked then the LAN2 interface will be listed. Similarly the loopback interface will be listed if it is enabled and configured. The network status with multiple interfaces is shown in Fig. 4.11 and with multiple interface including the loopback interface in Fig. 4.12.



Description	LAN	LAN2
Status	Up	Down
IP Address	10.10.70.91	192.168.1.100
Netmask	255.255.255.0	255.255.255.0
Packets Received	45,142	0
Bytes Received	4.95 MB	0 B
Packets Transmitted	14,238	0
Bytes Transmitted	4.99 MB	0 B

Fig. 4.11: LAN Status page with 2 LAN ports.



LAN

Description	Loopback	LAN	LAN2
Status	Up	Up	Down
IP Address	1.2.3.4	10.10.70.91	192.168.1.100
Netmask	255.255.255.255	255.255.255.0	255.255.255.0
Packets Received	0	45,315	0
Bytes Received	0 B	4.96 MB	0 B
Packets Transmitted	0	14,412	0
Bytes Transmitted	0 B	5.03 MB	0 B

Fig. 4.12: LAN Status page with loopback and 2 LAN ports.

4.4.1 LAN Statistics

Provides information of the LAN interfaces. Refer to Fig. 4.10 and Fig. 4.11.

Status
The status of the interface.

IP Address
The IP address of the interface.

Netmask
The netmask of the interface

Packets Received
The total number of packets received.

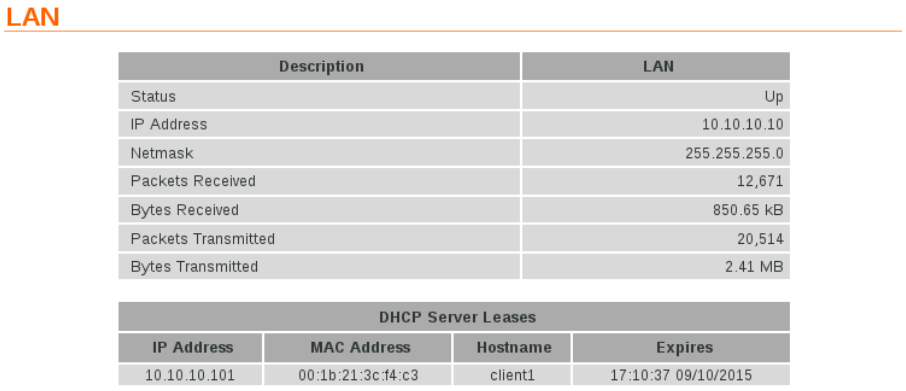
Bytes Received
The total number of bytes received.

Packets Transmitted
The total number of packets transmitted.

Bytes Transmitted
The total number of bytes transmitted.

4.4.2 DHCP Server Leases

The DHCP Server Leases section will only be shown if the DHCP server has been enabled. If the server has been enabled the LAN Status page will be similar to that shown in Fig. 4.13.



LAN

Description	LAN
Status	Up
IP Address	10.10.10.10
Netmask	255.255.255.0
Packets Received	12,671
Bytes Received	850.65 kB
Packets Transmitted	20,514
Bytes Transmitted	2.41 MB

DHCP Server Leases			
IP Address	MAC Address	Hostname	Expires
10.10.10.101	00:1b:21:3c:f4:c3	client1	17:10:37 09/10/2015

Fig. 4.13: LAN Status page with DHCP lease information.

IP Address
The assigned IP address.

MAC Address
The MAC address of the device which requested the lease.

Hostname
The reported host-name of the device which requested the lease.

Expires
The lease expiry time.

4.5 Routes

Display the routing table.

An example is shown in Fig. 4.14.

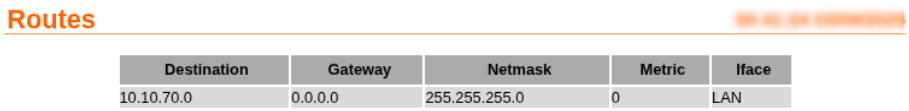


Fig. 4.14: The routing table.

The columns in the table are:

Destination
This is the address or network the route will target.

Gateway
The gateway to be used for packets that match the destination address or network.

Netmask
This is the network mask applied to the route.

Metric
The metric is used to determine which routing rule to use should there be more than one route possible.

Iface
The interface to which the packets matching the routing rule will be directed.

4.6 DNS

Display information on the currently configured DNS.

An example is shown in Fig. 4.15.

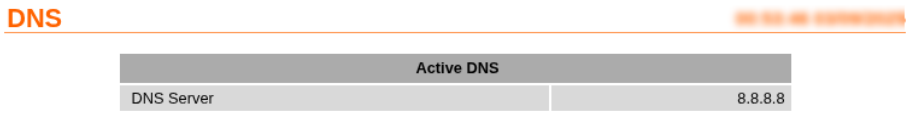


Fig. 4.15: Active DNS.

4.7 Virtual Private Network (VPN)

The Virtual Private Network (VPN) status page *Status→VPN* provides details of the current operating state of any configured Virtual Private Network (VPN). For details on VPN configuration refer to the *Virtual Private Network (VPN)* chapter.

4.7.1 IPsec Connection Status

Provides information on the state of any IPsec connections. Refer to Fig. 4.16

Label
The name given to the particular tunnel.

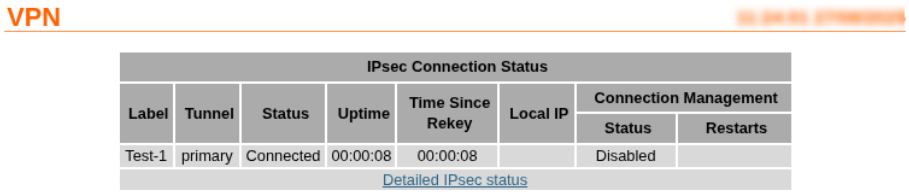


Fig. 4.16: VPN Status page showing IPsec connection status.

Tunnel
The tunnel type either Primary or Secondary.

Status
The connection status. When connected it will be reported as Connected.

Uptime
The time since the connection was established.

Time Since Rekey
The time since the last re-key.

Local IP
The local IP address if configured.

Connection Management
Connection management information:

Status
The current state of connection management.

Restarts
The number of connection management initiated re-starts.

4.7.2 Detailed IPsec Status

To display detailed logs of the IPsec connection click the link Detailed IPsec status below the status table. The log will be similar to that shown in Fig. 4.17.

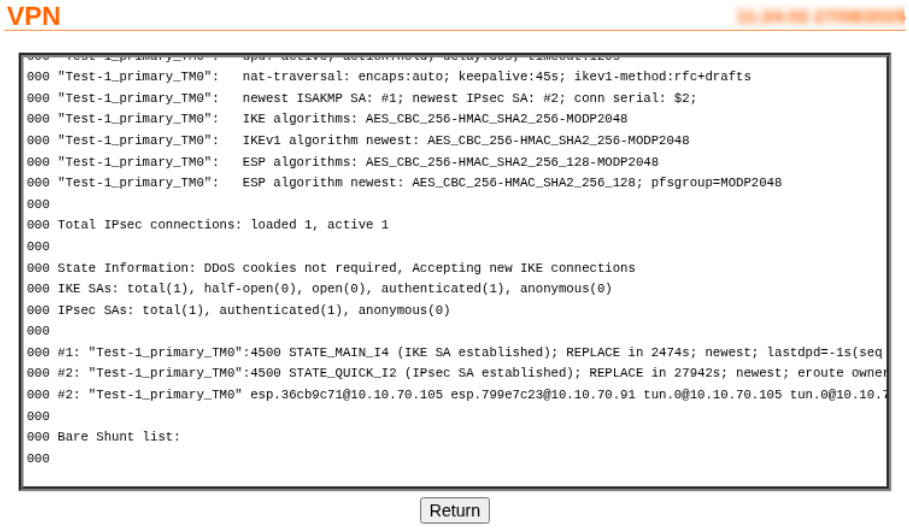


Fig. 4.17: Detailed IPsec connection status.

4.7.3 SSL Connection Status

Provides information on the state of any SSL VPN connections. Refer to Fig. 4.18.

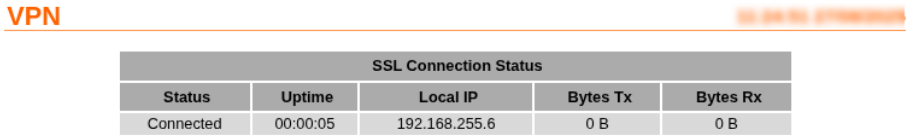


Fig. 4.18: VPN Status page showing SSL connections status.

Status
The connection status. When connected will report Connected.

Uptime
The time since the connection was established.

Local IP
The local IP address.

Bytes Tx
The number of bytes transmitted.

Bytes Rx
The number of bytes received.

4.7.4 PPTP/L2TP Connection Status

Provides information on the state of any PPTP/L2TP connections. Refer to Fig. 4.19.

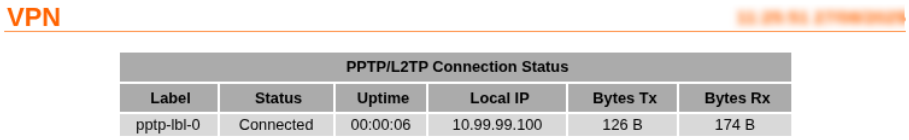


Fig. 4.19: VPN Status page showing PPTP/L2TP connections status.

Label
The label assigned to the VPN during configuration.

Status
The connection status. When connected will report Connected.

Uptime
The time since the connection was established.

Local IP
The local IP address.

Bytes Tx
The number of bytes transmitted.

Bytes Rx
The number of bytes received.

4.7.5 Multiple VPN Connection Status

If more than one VPN is configured, including different VPN types, the page will expand to include tables and entries all of the tunnels.

For example If both IPsec and SSL VPN connections are configured both be displayed as shown in Fig. 4.20.

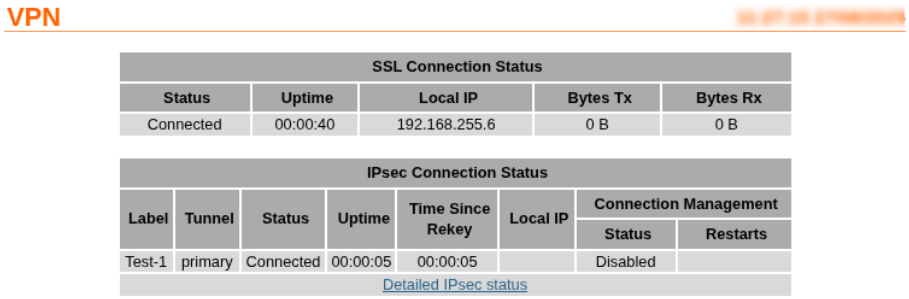


Fig. 4.20: VPN Status page showing both IPsec and SSL connection status.

4.8 Generic Routing Encapsulation (GRE)

The Generic Routing Encapsulation (GRE) status page *Status→GRE* provides details of the current operating state of any configured GRE tunnels.

For GRE settings refer to Section *Generic Routing Encapsulation (GRE)* in the *Network* chapter.

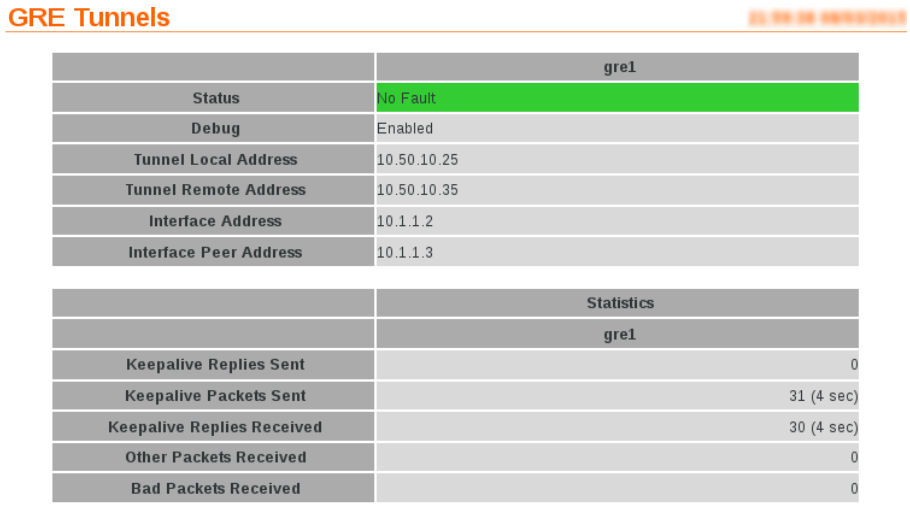


Fig. 4.21: GRE Status page.

4.8.1 GRE Tunnel Details

The first section provides details for all configured GRE tunnels. The tunnel label is listed at the top of the column. In Fig. 4.21 the details of the tunnel labelled 'gre1' are shown.

Status
: The operating status of the tunnel. When established and operating correctly it will be reported as No Fault.

Debug
: The debug state. Reported as:

  Enabled
  : When debug is enabled; or

Disabled
When debug is not enabled.

Tunnel Local Address
The local IP address of the tunnel.

Tunnel Remote Address
The remote IP address of the tunnel.

Interface Address
The IP address of the interface over which the tunnel will be established.

Interface Peer Address
The IP address of the remote interface over which the tunnel will be established.

4.8.2 GRE Tunnel Statistics

The section section of the table details the statistics of the configured GRE tunnels.

Keepalive Replies Sent
The number of keep-alive replies sent in response to keep-alive packets received.

Keepalive Packets Sent
The number of keep-alive packets sent to the remote interface.

Keepalive Replies Received
The number of keep-alive replies received in response to keep-alive packets sent.

Other Packets Received
The number of packets received excluding keep-alive packets.

Bad Packets Received
The number of errored packets received.

4.9 Serial Server

The Serial Server status page *Status→Serial Server* provides details of the current operating state of any serial ports configured to work with the serial server.

For details on configuring the Serial Server refer to the *Serial Server* chapter.

The status page contains 1 column for each serial port of the unit, Fig. 4.22 shows the page for a unit with 1 serial port and Fig. 4.23 shows the page for a unit with 3 serial ports.

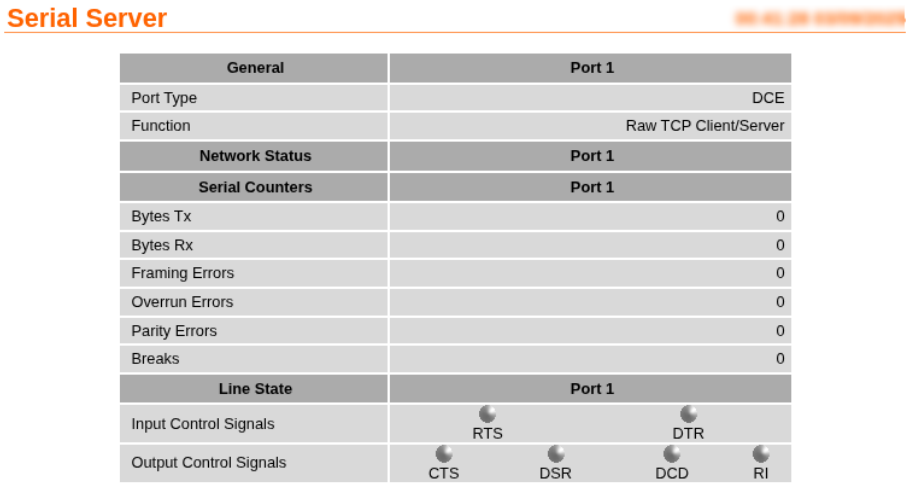


Fig. 4.22: Serial Server Status page for unit with 1 serial port.

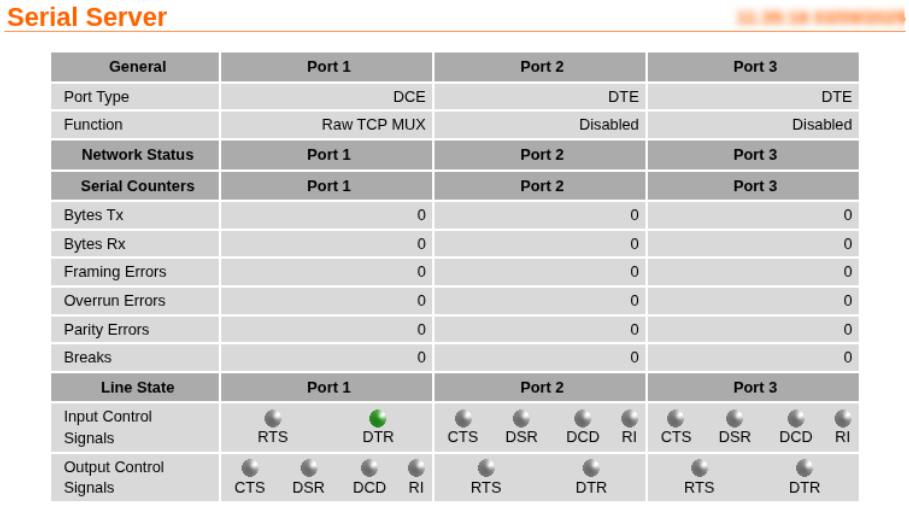


Fig. 4.23: Serial Server Status page for unit with 3 serial ports.

4.9.1 Status Description

Description of the Serial server status table.

General

Port Type
The type of serial port.

Function
Configured function of the port.

Network Status

Network State
Operating state of the port, either Connected or Disconnected.

Remote Address
The IP address of the connection. Shown only when connected.

Uptime
The time since the connection was established.

Serial Counters

Bytes Tx
The number of bytes transmitted since the connection was established.

Bytes Rx
The number of bytes received since the connection was established.

Framing Errors
The number of receiver framing errors.

Overrun Errors
The number of receiver overrun errors.

Parity Errors
The number of receiver parity errors.

Breaks
The number of receiver breaks.

Line State

Report of the current state of all signal lines. The indicator is green when asserted and grey when de-asserted.

Input Control signals

RTS
Ready To Send.

DTR
Data Terminal Ready.

Output Control signals

CTS
Clear To Send.

DSR
Data Set Ready.

DCD
Data Carrier Detect.

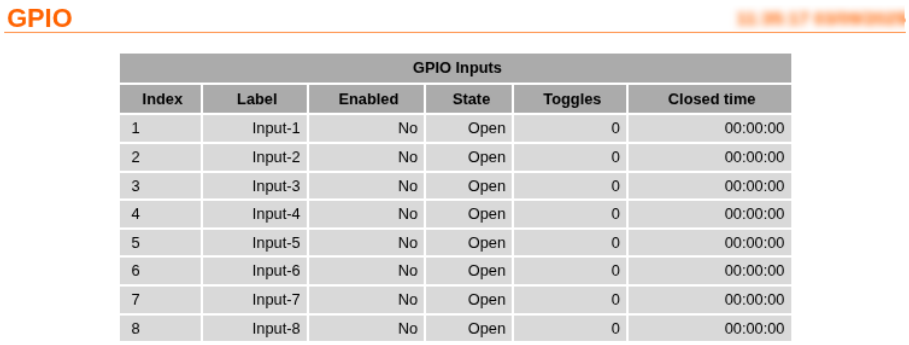
RI
Ring Indicate.

4.10 General Purpose Input / Output (GPIO)

The General Purpose Input / Output *Status→GPIO* provides details of the current operating state of any GPIO for the device.

An example of the GPIO status page is shown in Fig. 4.24.

For GPIO settings refer to Section *General Purpose Inputs and Outputs (GPIO)* in the *System* chapter.



GPIO Inputs					
Index	Label	Enabled	State	Toggles	Closed time
1	Input-1	No	Open	0	00:00:00
2	Input-2	No	Open	0	00:00:00
3	Input-3	No	Open	0	00:00:00
4	Input-4	No	Open	0	00:00:00
5	Input-5	No	Open	0	00:00:00
6	Input-6	No	Open	0	00:00:00
7	Input-7	No	Open	0	00:00:00
8	Input-8	No	Open	0	00:00:00

Fig. 4.24: GPIO Status page.

4.10.1 GPIO Inputs

Provides information on the current state and past closures of the GPIO inputs.

Index
The number of the input starting at 1 for the first input.

Label
The configured label for the input.

Enabled
The current state of the input either:

Yes
Enabled; or

No
Disabled.

State
The current state of the input either Closed (Active) or Open.

Toggles
The number of times the input has toggled to the closed state.

Closed time
The total accumulated time for which the input has been closed.

4.10.2 GPIO Outputs

Provides information on the current state and past closures of the GPIO inputs.

Index
The number of the output starting at 1 for the first output.

Label
The configured label for the output.

Enabled
The current state of the output either:

Yes
Enabled; or

No
Disabled.

State
The current state of the output either Closed (Active) or Open.

Toggles
The number of times the output has toggled to the closed state.

Closed time
The total accumulated time for which the output has been closed.

4.11 System Logs

The System Logs page *Status→System Logs* provides access to diagnostic and operational information recorded by the unit. Users may select between 'System', 'Location' or Serial Trace logs from the drop-down list to view different types of logged information.

4.11.1 System Log

The system log provides a list of messages from various services. The messages are time and date stamped. The page will display up to 1,000 lines of the log file. As the logs are persistent once the unit has been operating long enough for the log to contain at least 1,000 lines the page will consistently display 1,000 lines.

An example of the System Logs page is shown in Fig. 4.25.

4.11.2 Location Log

The location log provides a record of the device's location information.

If GNSS is enabled and the log option has been enabled, then log entries will appear similar to the following:

```
<timestamp>: Location: 33 Degrees 49.147' S 151 Degrees 7.470' E
<timestamp>: Location: 33 Degrees 49.147' S 151 Degrees 7.470' E
```

Where:
<timestamp>: Is the timestamp in the form dd/mm/yyyy hh:mm:ss timezone.

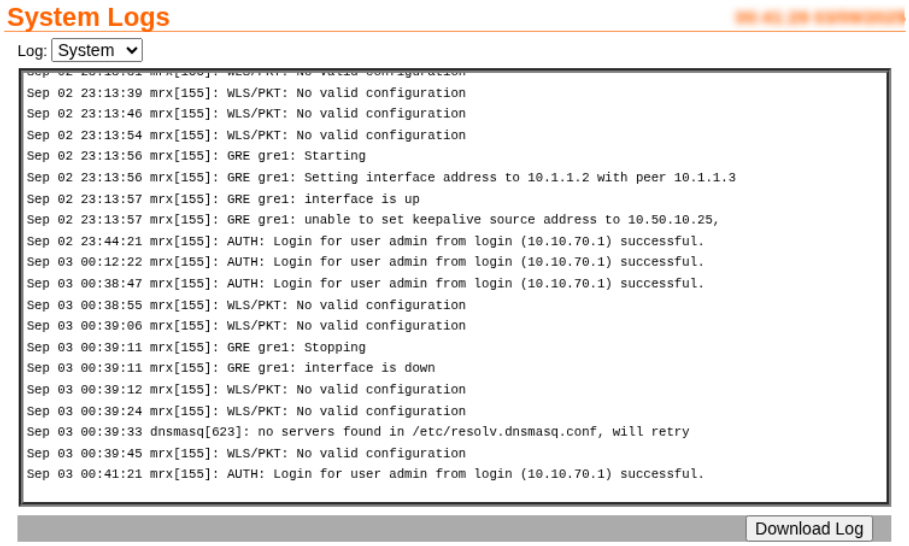


Fig. 4.25: System Log page.

4.11.3 Serial Trace

The serial trace shows the octets transmitted and received on a serial port. The log includes a timestamp the serial port number and the direction RX or TX. The octets are listed as hex values and the character represented by the octet is also shown if printable.

An example of a serial trace is:

```
<timestamp>: Port 1 RX: 6 bytes
00000000 c0 7e 28 57 48 13                                        :.~(WH.
<timestamp>: Port 1 RX: 3 bytes
00000000 dd 48 6c                                                 :.Hl
<timestamp>: Port 1 RX: 6 bytes
00000000 a0 55 54 c0 1f ce                                        :.UT...
<timestamp>: Port 1 RX: 3 bytes
00000000 f4 cc c7                                                 :...
<timestamp>: Port 1 RX: 1 bytes
00000000 42                                                       :B
```

Where:

<timestamp>: Is the timestamp in the form dd/mm/yyyy hh:mm:ss (timezone)

4.11.4 Log Download

All logs can be downloaded from the unit as plain text files by first selecting the required log then clicking the Download Log link at the bottom right of the page. The downloaded file will be up to 1 Mbyte in size.

> **Note**
>
> Due to the way in which the log files are rotated once the unit has been operating for some time to downloaded file will be between 500 Kbytes and 1 Mbyte in size.

CHAPTER

FIVE

SYSTEM

The System tab section provides configuration options and access to features to related to the administration and system level configuration of the unit.

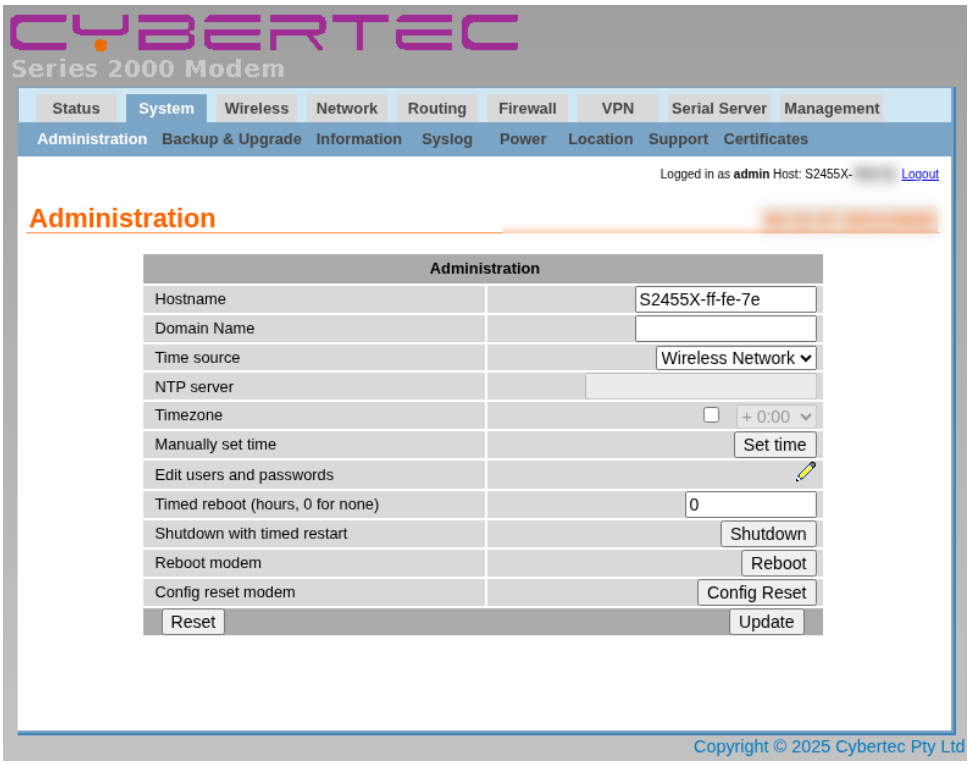


Fig. 5.1: The main System administration page.

Options which can be configured include:

- Host-name for the device.
- Domain name.
- Time and Date settings.
- Edit users and passwords
- RADIUS server.
- Shut-down and re-boot.
- Reset the configuration of the unit to the default configuration.
- Save and restore the device configuration.
- Update the device firmware.
- View device information, serial number, MAC address etc.

- Power controller.
- General Purpose Input and Output (GPIO).

The System pages are accessed by clicking System on the main menu.

5.1 Administration

The main Administration page is the default page and will be displayed when System is selected from the main menu. It can also be selected by the menu combination *System →Administration* at any time. A page similar to that shown in Fig. 5.1 will be displayed.

5.2 System Configuration

The System configuration options are accessed from the main System Administration page. Fig. 5.2 is an example of the page.

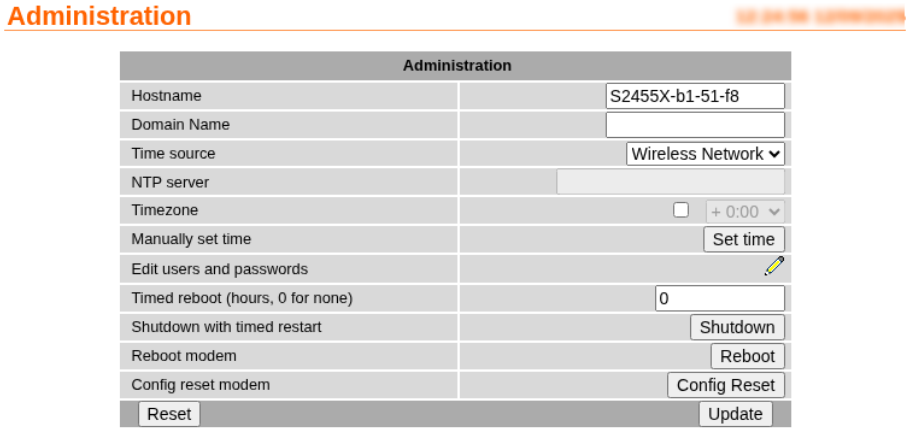


Fig. 5.2: The main System administration configuration page.

5.2.1 Setting the system host-name

The host-name for the modem can be set in the Hostname field. The host-name is limited to 32 characters and can only contain letters 'a' through 'z' and 'A' through 'Z', digits '0' through '9' and hyphens '-', no other symbols, punctuation characters, or white space are permitted. The host-name is displayed on this page, reported via SNMP and used in system-generated SMS messages.

The default host-name is '<model>-<xx-xx-xx>'

Where:

model
: is the device model designation, and

xx-xx-xx
: is the last 3 octets of the unit's MAC address.

Note

As this host-name is based on the MAC address of the unit it will be unique.

5.2.2 Domain Name

The domain name for the modem can be set in the Domain Name field. The domain name is limited to 64 characters and can contain letters 'a' through 'z' and 'A' through 'Z', digits '0' through '9', hyphens '-', and periods '.', no other symbols, punctuation characters, or white space are permitted. The domain name is displayed on this page and reported via SNMP.

5.2.3 Selecting the Time Source

Time Source

The time source is selected from the 'Time source' drop-down box.

The options are:

Wireless Network

Use the 3G/4G connection for the time source. (Default)

NTP

Network Time Protocol

Manual

The time and date are set manually with no external time synchronisation.

If the default option of Wireless Network is selected no further configuration is required, if either of the other options is selected further configuration will be required.

5.2.4 Using the Network Time Protocol (NTP)

The time source may be configured to read the current time from a network time server using the NTP protocol. To enable NTP, select NTP from the Time source drop-down box and then enter the IP address or host-name of an NTP server in the text field. To correctly adjust the time from the NTP server to the local time zone, the Timezone must be set. Select the appropriate number of hours for the time zone in which the unit will be operating, from the drop-down list.

5.2.5 Manual Setting of the time and date

To manually set the time select Manual from the Time source drop-down box and then click the button, a pop-up box will be displayed similar to that shown in Fig. 5.3. Adjust the time and date to the desired settings and click the Set button to save.

Fig. 5.3: Manually setting the time and date.

Note

When the time source is set to Manual no external synchronisation will be performed. This means the internal Real Time Clock (RTC) could drift and so not report the correct time. If the unit is left un-powered for such time as the RTC power source is lost the time settings will also be lost.

5.2.6 Enable Local NTP Server

Enable the NTP server to provide NTP time services to local devices.

5.2.7 Editing users and passwords

To change the passwords used for modem access or to enable RADIUS authentication, click the  icon in the Edit users and passwords field. A page similar to that shown in Fig. 5.4 will be displayed.

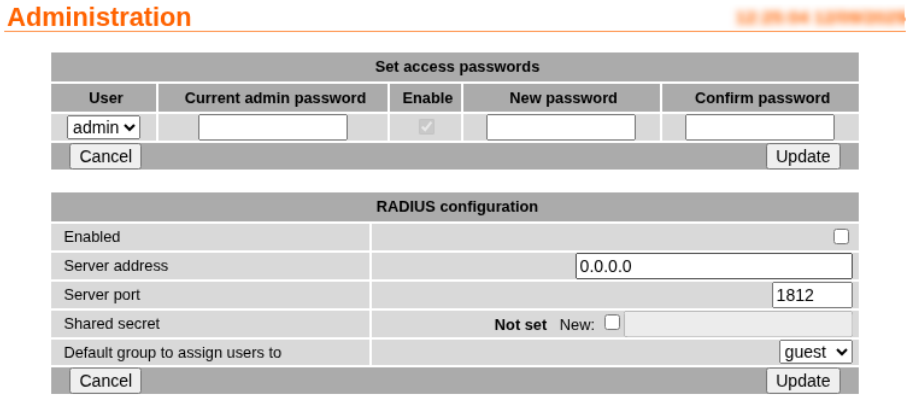


Fig. 5.4: Administration page to change user passwords and to configure RADIUS.

5.2.8 Changing user passwords

There are two users, each with different access levels:

Access Level:

admin
: The admin user can view and change the configuration of the modem and view the status.

guest
: The guest user can view the configuration and status of the modem. This user is disabled by default.

> **Note**
>
> The admin user is enabled by default. The guest user is not enabled by default, to enable the guest ensure the Enable check-box is checked.

The passwords for both users are set using the **Set access passwords** table.

To change a user's password, use the drop-down box in the **User** column to select the appropriate user. Then, enter the **Current password** for the user, followed by the **New password**, repeated to avoid errors in the Confirm password field.

To enable the guest user check the **Enabled** check-box. Click the Update button to confirm and save the changes.

5.2.9 Configuring RADIUS authentication

User credentials can also be authenticated against a RADIUS server. The fields below need to be correctly configured to enable this feature. The RADIUS server administrator will be able to provide the necessary information.

RADIUS Configuration:

Enabled
: Set this field to enable RADIUS authentication.

Server address
Enter the IP address of the RADIUS server.

Server port
Enter the IP port of the RADIUS server. This is normally 1812 or 1645.

Shared secret
This is a password that is used to encrypt traffic sent to the RADIUS server. To set this field, click the **New** check-box and enter the secret in the text field.

Default group to assign users to
If the RADIUS server fails to provide information regarding the access level of a newly authenticated user, the default set in this field will be used.

> **Note**
>
> RADIUS attribute Service-Type (6) is used to determine the access level of a user. A user with Service-Type set to Administrative-User (6) will be granted the admin access level. A user with Service-Type set to NAS-Prompt (7) will be granted the guest access level.

Click the Update button to confirm and save the changes.

5.2.10 Setting a timed reboot

In some applications, it may be desirable for the unit to re-boot at a timed interval. To enable this feature, enter a time (in hours) in the Timed reboot field. Once the modem has run for the number of hours entered, it will reboot and start the system again. To disable this feature, set the field to 0.

> **Note**
>
> The use of the timed reboot feature is not recommended. The device continuously monitors the operating conditions and network status, if a fault is detected corrective action is taken in order to re-establish network connections. Using the connection management features details in Section 6 will provide a more reliable and stable solution.

5.2.11 Shutdown

A shut-down can be initialised by clicking the Shutdown button, this is recommended before removing power. A shutdown will disconnect the device from any network to which it is connected, terminated all processors and close all connections, the power supplies will then be turned off. The complete shutdown will take approximately 2 minutes. The power will remain off for approximately 1 minute, during this time the power can safely be removed. After this time if the power is still connected the device will start up again and resume normal operation.

> **Note**
>
> It is recommended to shutdown the unit using the method described before removing the power.

5.2.12 Rebooting the modem

A re-boot can be initiated by clicking the Reboot button and then confirming the action when the pop-up dialogue box that appears. The reboot will take around 75 seconds.

> **Note**

The power supplies remain on during a reboot, this differs from a shutdown where the power supplies are turned off.

5.2.13 Configuration reset modem

The configuration of the modem can be reset to the default values by clicking the Config Reset button and then confirming the action when the pop-up dialogue box that appears. The unit will then reboot.

Warning

The configuration of the unit will be reset to the default values, this includes the IP address of the unit and the passwords.

To access the unit after reset the default IP address should be used.

Note

This option is guaranteed to delete all configuration data only.

5.2.14 Factory reset modem

To factory reset the unit click the button Factory Reset. This will delete all configuration, certificates and logs from the unit.

5.2.15 Update & Reset

After completing configuration changes, click the Update button to apply all changes.

5.3 Backup & Upgrade

This section describes how to save the current modem configuration, restore a saved configuration and update the firmware. To access the Backup & Upgrade options select *System* → *Backup & Upgrade*. The Backup & Upgrade page will be displayed as shown in Fig. 5.5.

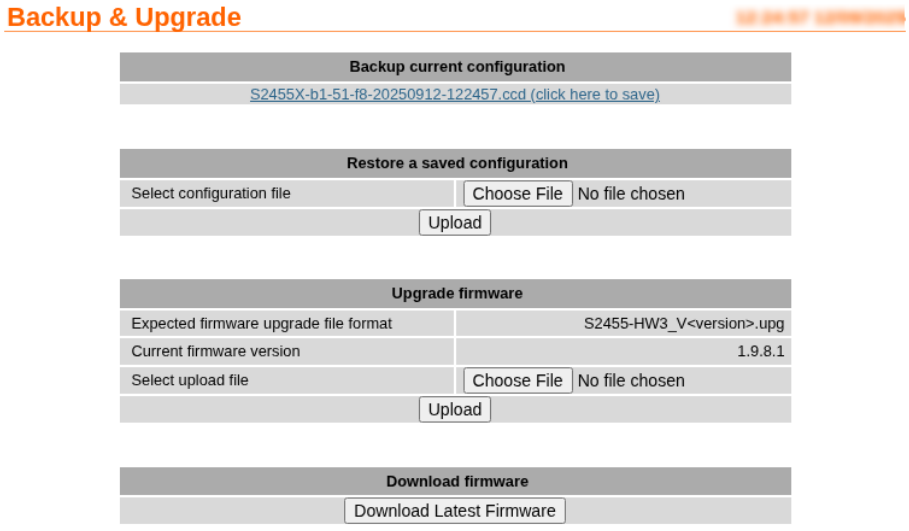


Fig. 5.5: System Backup and Upgrade page.

5.3.1 Backing up the current configuration

The configuration can be downloaded and saved as a file, this file can then be used to restore the configuration of the unit at some later time or used to configure multiple units with the same configuration. Click on the link in the section titled **Backup current configuration** to download the current configuration.

The file-name is in the format <Host-name>-<Date>-<Time>.ccd

Where:

Host-name
is the host-name for the unit. Refer to Section <Hostname> for details.

Date
is the current date in the format YYYYMMDD where:

YYYY
is the year

MM
is the month

DD
is the day

Time
is the time in the format HHMMSS, where:

HH
is the hour

MM
is the minute

SS
is the seconds

.ccd
is the file type. (Configuration file).

> **Warning**
>
> The filename for the configuration file is set when the page is first loaded and will remain as long as the page is not refreshed. The file-name will be updated each time the page is refreshed.

5.3.2 Restoring a saved configuration

To restore a configuration, click the Choose file button in the section titled Restore a saved configuration. Select the configuration file, which will then be shown in the text box, as shown highlighted in Fig. 5.6. Click the Upload button to transfer the file to the unit.

Once uploaded the unit will need to be rebooted, in order for the uploaded configuration to be applied. A warning will be shown indicating the unit will need to be rebooted for the uploaded configuration to be applied.

> **Warning**
>
> Do not change any configuration settings until the modem has been rebooted.
>
> Any changes required should be made after the unit has been rebooted.
>
> If a configuration setting is changed prior to reboot the current running configuration will be written over-writing the uploaded configuration file.

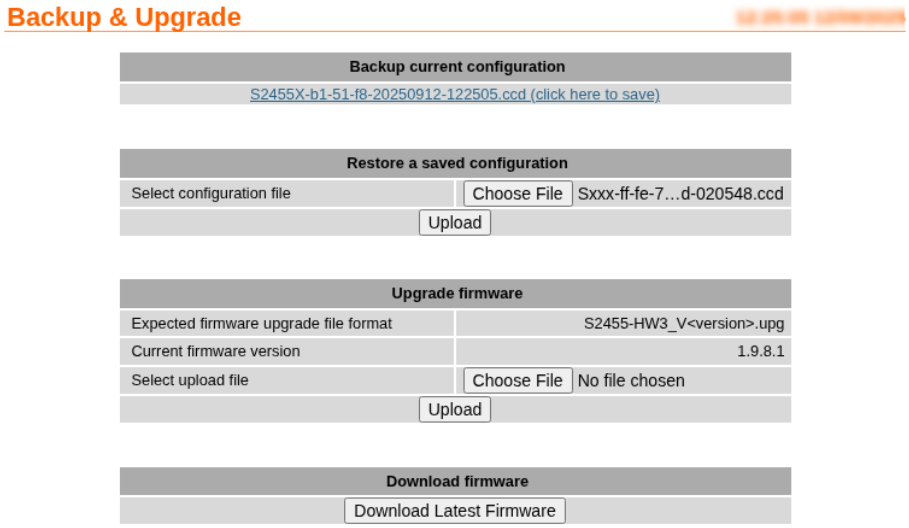


Fig. 5.6: Restore configuration.

5.3.3 Upgrading the modem firmware

The firmware can be upgraded via the web interface. To upgrade the firmware, click the button in the section titled Upgrade firmware then navigate to and select the upgrade file. Once selected, the file-name will display as shown highlighted in Fig. 5.7.

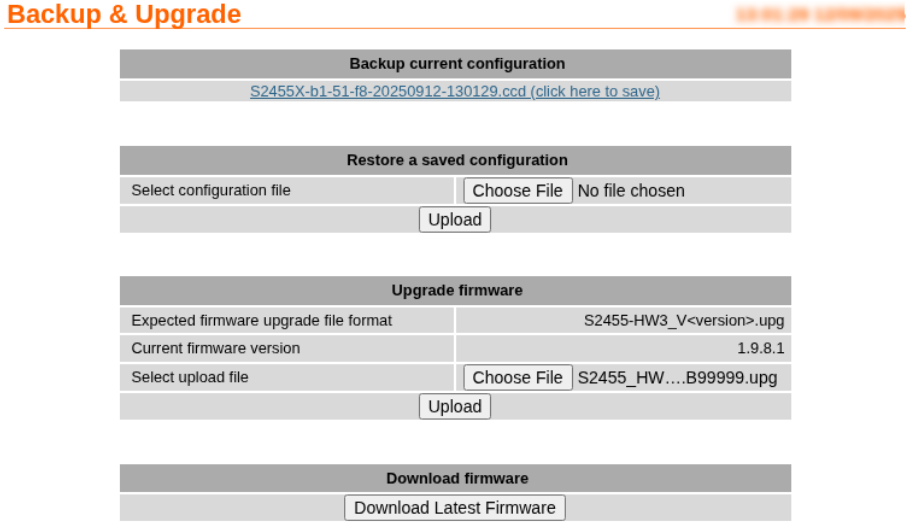


Fig. 5.7: Firmware upgrade choose file.

To initiate the upload of the file click the Choose File button, the file will now be uploaded. The upload may take from several seconds to several minutes depending on the speed of the link the upgrade file is transferred over. When the upload is complete, information on the upgrade file will be displayed, as shown in Fig. 5.8.

To proceed with the upgrade click the Upgrade button. The upgrade process will now proceed.

The upgrade can be cancelled by clicking the Cancel button.

Warning

The upgrade will take several minutes to complete after which time the unit will reboot.

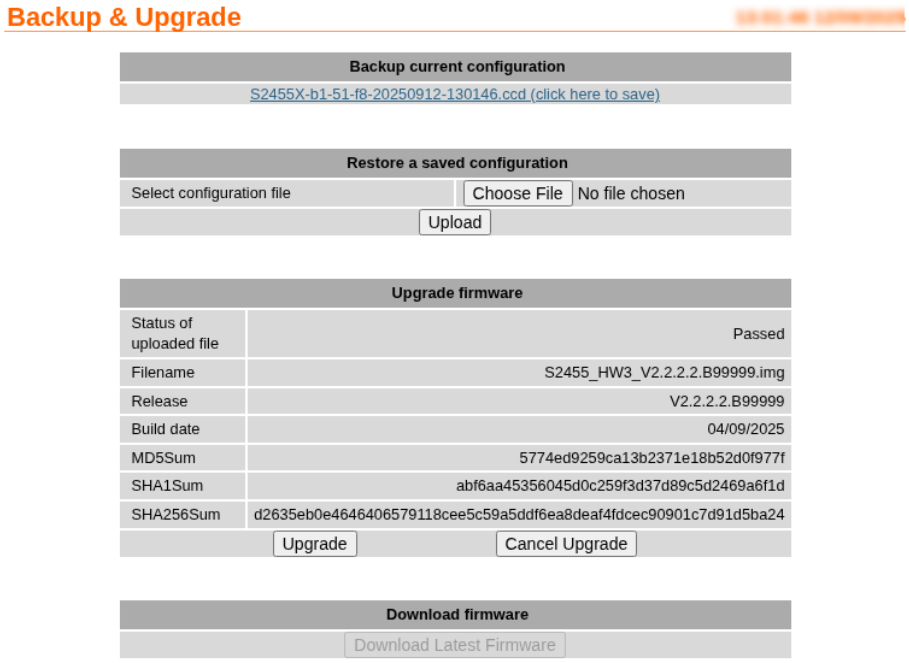


Fig. 5.8: Start firmware upgrade.

During this time the power to the unit must not be removed.

If power is removed during this time the unit may not re-boot.

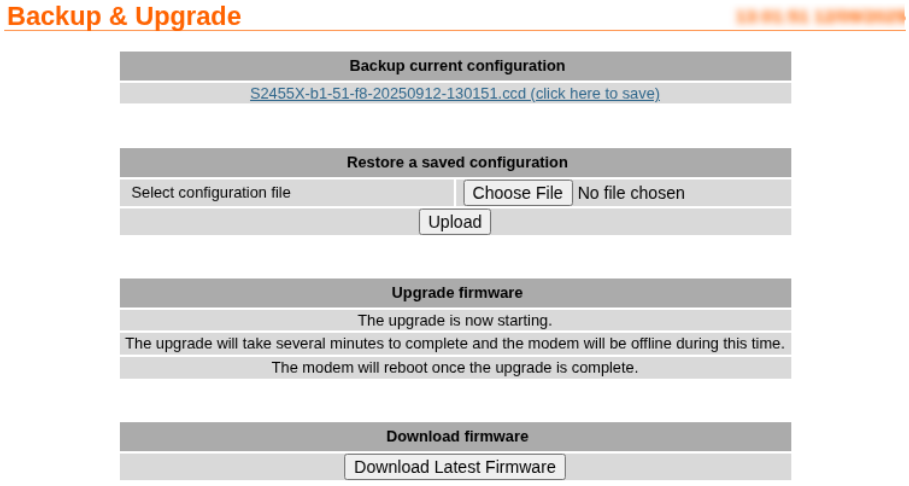


Fig. 5.9: Firmware upgrade in progress.

Once the firmware upgrade has completed the unit will re-boot and the web pages will again be accessible.

5.3.4 Download firmware

The latest firmware for the unit can be downloaded by clicking the button **Download firmware**.

5.4 System Information

System Information is accessed by selecting menu *System* → *Information*. An example of the System Information page is shown in Fig. 5.10.

The first section of the page lists the model and serial number of the unit, plus the firmware and boot loader version. The second part of the page lists the LAN MAC address the IMEI of the wireless module and the wireless IMSI.

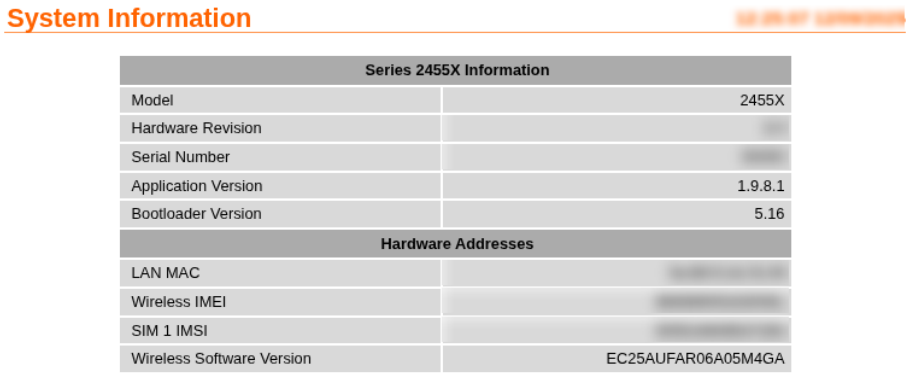


Fig. 5.10: System information page.

5.4.1 Unit Information

The first section of the page lists the following:

Unit Information:

Model
The model number of the unit.

Hardware Revision
The hardware revision of the unit.

Serial Number
The serial number of the unit.

Application Version
The application firmware version currently installed.

Bootloader Version
The bootloader firmware version currently installed.

5.4.2 Hardware Addresses

The second part of the page lists the hardware address of the unit as follows:

Hardware Addresses

LAN MAC
The LAN Media Access Control (MAC) address assigned to the Ethernet port of the device.

Wireless IMEI
The International Mobile Station Equipment Identity (IMEI) number of the wireless interface.

SIM n IMSI
The International mobile subscriber identity (IMSI) read from the SIM card.

Wireless Software Version
The wireless (or RF) firmware version currently installed.

> **Note**
>
> The SIM IMSI will only be listed if an SIM is inserted and can be accessed.
>
> If the unit supports more than one SIM then the IMSI for the active SIM will be reported.

5.5 Syslog

Syslog allows the logs to be sent to a remote system for storage and analysis. The Syslog page is accessed by selecting *System* → *Syslog*. A page similar to that shown in Fig. 5.11 will be shown.

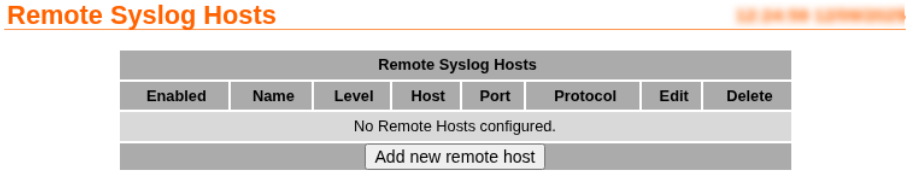


Fig. 5.11: The default Syslog page.

5.5.1 Adding a Remote Syslog Host

To add a remote Syslog host click the Add new remote host button, a page similar to that shown in Fig. 5.12 will be displayed.

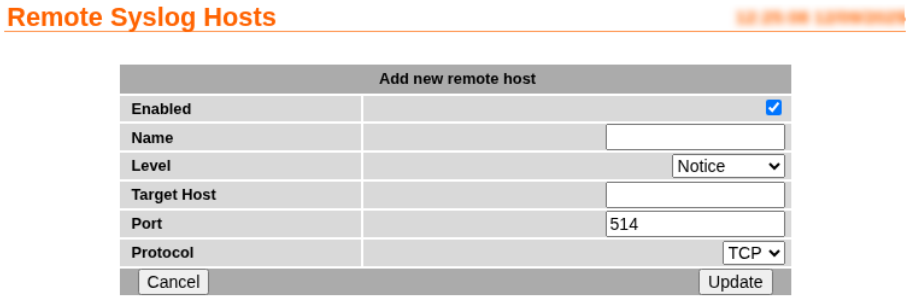


Fig. 5.12: Add a remote Syslog host

To add a new host the following fields are required:

Syslog Configuration

Enabled
Check to enable Syslog to this remote host.

Name
The name or label for this remote syslog.

Level
The logging level. The logging levels are:

Info
Informational logs include information about successful operations within the system, such as a successful interface connection or a service start or stop.

> **Note**
>
> This level may generate a large number of messages.

Notice (Default)
Notice logs include information about events that may be unusual but are not errors. Notice logs are technically normal, but still significant enough to have their own severity level between information and warning.

Warning
Warning conditions are slightly less severe than error conditions. Error conditions happen when an operation fails, while a warning might indicate that an operation will fail in the future if action is not taken now.

Error
This category is assigned to event logs that contain a system error message.

Critical
Critical log category is for critical errors, such as hardware failure.

Alert
Alert logs are assigned when an event log requires an immediate response to prevent the loss of service.

Emergency
The highest level, emergency messages only. Very few messages at this level.

Target Host
The IP address or host-name of the remote Syslog server.

Port
The TCP/IP port to use for the connection.

Protocol
Select the protocol to use for the connection, either UDP or TCP (Default)

Once complete click Update To save the changes.

> **Note**
>
> The lower the logging level the higher the number of log messages.

> **Warning**
>
> Setting the level too high may affect performance particularly if the bandwidth available is limited.

5.5.2 Example of Adding a Remote Syslog Host

In this example a new remote host will be configured with the details shown in Fig. 5.13.

After clicking the Update button, the main Syslog page is shown again with the new remote Syslog host listed, as shown in Fig. 5.14.

Additional hosts may be added by following the same procedure.

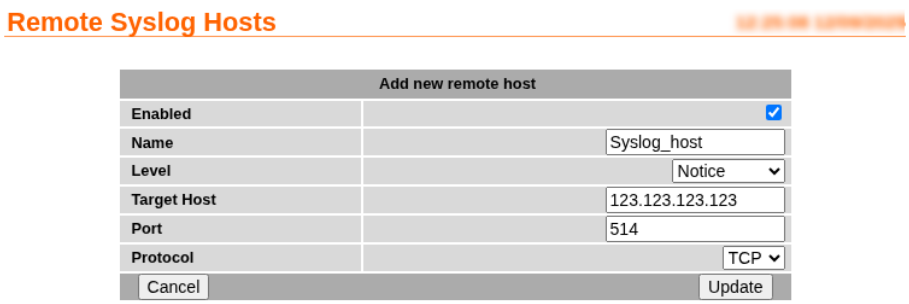


Fig. 5.13: Example of adding a remote Syslog host.

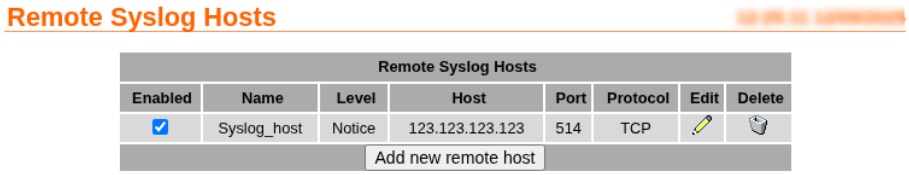


Fig. 5.14: Main Syslog page showing new remote host.

5.5.3 Editing Remote Syslog Host

To edit a Remote Syslog host click the  icon beside the entry in the table. The details for the entry will be displayed in a page the same as for the add remote Syslog host. The details can be modified and saved by clicking Update

5.5.4 Deleting a Remote Syslog Host

To delete a Remote Syslog host click the  icon beside the entry in the table. A confirmation dialogue will appear, click OK to delete or Cancel to cancel the deletion.

5.6 Power

The power controller may be used to power the unit on and off at specified times. By using the power controller the power consumption can be greatly reduced at times when a network connection is not required. The power controller options are on *System* → *Power* page, which is shown in Fig. 5.15.

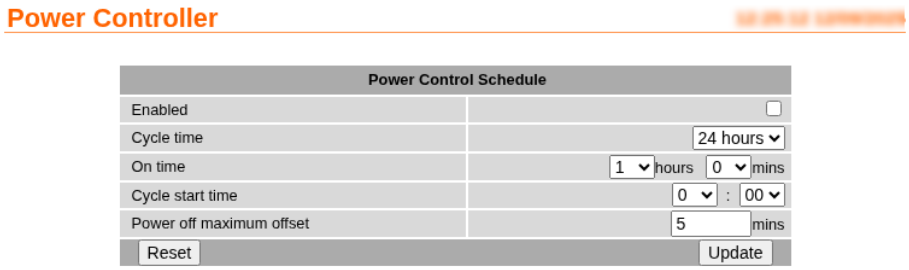


Fig. 5.15: The Power Control Schedule configuration page.

For the power controller to work correctly power must be maintained to the unit at all times. During the power off times the power consumption will drop to a low level which will vary between models. This power is required to maintain the timer circuitry which determines when the unit should again be powered on. If during an power off time the power is removed from the unit the timer count is lost. When power is re-applied the unit will boot as normal, the timer will be re-initialised and determine if it should remain powered on or enter the power off state.

5.6.1 Configuring Power Control Schedule

The configuration options are:

Enabled
Enable the power controller by checking the box.

Cycle time
Select the required cycle time from the drop-down list.

On time
Select duration for which the power is on.

Cycle start time
Select the time, offset from start of the cycle, at which the power is turned on.

Power off maximum offset
If enabled, specifies an offset time which is applied if the unit re-powers prior to the scheduled power on time.

The controller works on the basis of a cycle, the duration of the cycle can be set for a maximum of 24 hours to a minimum of 30 minutes. Irrespective of the cycle duration the first cycle begins at midnight subsequent cycles begin straight after the previous cycle. For example if the cycle time is set to 6 hours, the first cycle starts at 12:00am, the second at 06:00am, the third at 12:00pm, the forth at 6pm and so on.

The period for which the unit is powered is set as the on time this time can be set to a maximum of 5 minutes less then the cycle time. If this value is set to 0 in will default to the maximum on time of 5 minutes less than the cycle time. The time at which the powered duration begins relative to the start of the cycle is specified as the cycle start time. For example if the On time is set to 30 minutes and the Cycle start time is set to 1 hour the unit will be off for the first hour of the cycle, it will then be powered on for 30 minutes and then remain off for the rest of the cycle. Once the configuration has been completed click the Update button to save and commit the changes.

5.6.2 Power Control Schedule Example

Example 1

The unit is required to be powered on at 2:00am and again at 2:00pm for a duration of one hour.

As there are two power on times per day the cycle time required is 12 hours. The On time is 1 hour and the Cycle start time is 2 hours. The required settings are shown in Fig. 5.16.

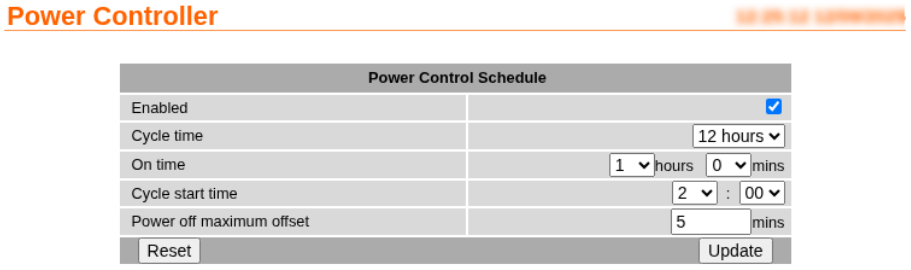


Fig. 5.16: Power Control Schedule configuration example 1.

Example 2

The unit is required to be powered on from 5:45am to 6:15am each day. If the power to the unit fails and is returned at 5:30am or later it is to remain on until normal power off time.

In this example as the unit is only powered once per day the Cycle time required is 24 hours. The On time is the duration from the power on time and the power off time which is 30 minutes. The Cycle start time is 5 hours and 45 minutes which is the time from midnight to the power on time. The Power maximum offset is enabled and the time set to 15 minutes. The configuration is shown in Fig. 5.17.

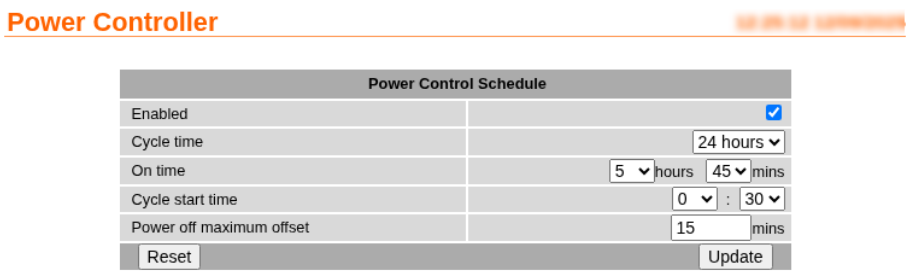


Fig. 5.17: Power Control Schedule configuration example 2.

5.7 General Purpose Inputs and Outputs (GPIO)

The General Purpose Inputs and Outputs (GPIO) provide a way in which to monitor and control external devices. The inputs may be used to trigger events such as sending an SMS, email or SNMP trap. The outputs can be changed as a result of an event such as the receipt of an SMS. The GPIO options are on *System* → *GPIO* page, which is shown in Fig. 5.18.

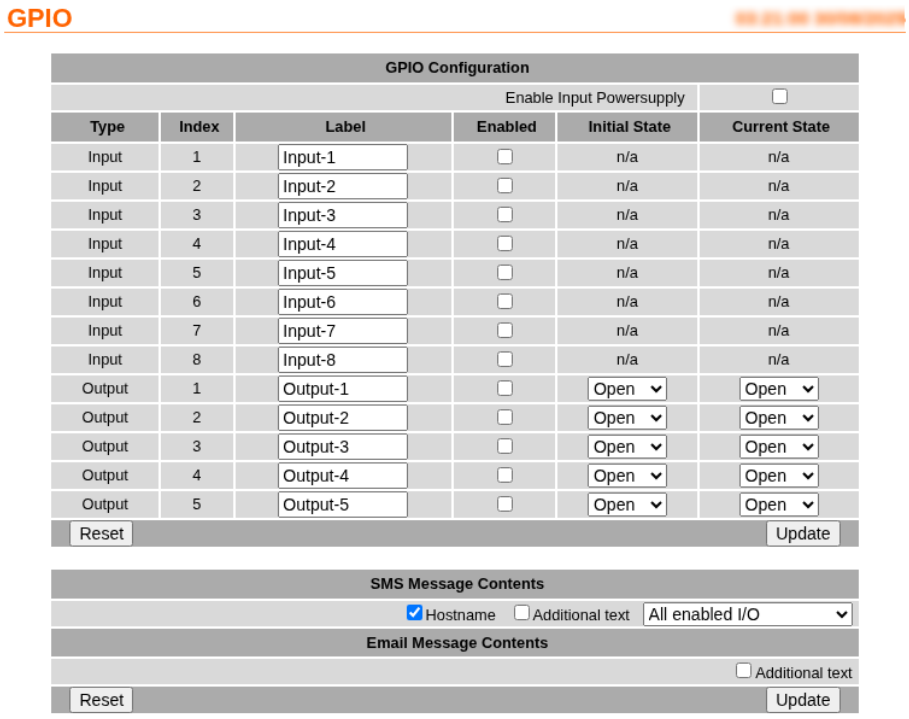


Fig. 5.18: The GPIO configuration page.

5.7.1 GPIO Configuration

The GPIO Configuration of the page is used to configure the individual inputs and outputs.

Enable Input Power Supply
: Check this box to enable the power supply to power the input circuitry. This is required if the inputs are to work as closed contacts. If the inputs will be triggered with a voltage input this power supply can remain off.

The options within the table are:

Type
: This field describes the I/O type and is one of:

  Input
  : The I/O is an input.

Output
The I/O is an output.

Index
This is the index of the I/O and is referenced for each type. This index matches the hardware index for the I/O.

Label
A text label for the I/O.

Enabled
Check to enable reporting of the Input or Output.

Initial State
This is the initial state the output will transition to when the unit powers up or re-boots. This field is not applicable for inputs. The state can either be:

Open
The output is in the open or off state.

Closed
The output is in the closed or on state.

Once the configuration has been completed click the Update button to save and commit the changes.

Note

The state of the outputs when the unit is powered off and when it commences the boot process will be open. The default state will be applied during the boot sequence. This means that if an output is set to a default state of Closed then it will initially be Open then transition to Closed during power up.

Note

When the unit is powered off or in low power mode, refer to Section *Power* the outputs will be in the Open state.

5.7.2 General Configuration

The general configuration is used to configure the way in which the unit will respond to an I/O event.

The options are:

SMS Message Contents
Should an input or output cause an SMS event to be generated, the values set in these fields determine the contents of the message. The values are:

Hostname
Check to include the unit host-name in the message.

Additional text
Check to include additional text to be included in the message. When checked a text box will be appear containing the additional text to include in the message, as shown in Fig. 5.19. To add or edit text click the  icon beside the text box, an example is shown in Fig. 5.20.

When to Send
Drop-down box with options for when to send and what to include in message.

Select from:

No I/O
No I/O state included in the message

I/O that generated event
Only the state of input or output which generated the event will be included in the message.

All enabled I/O
The state of all enabled inputs and outputs will be included in the message.

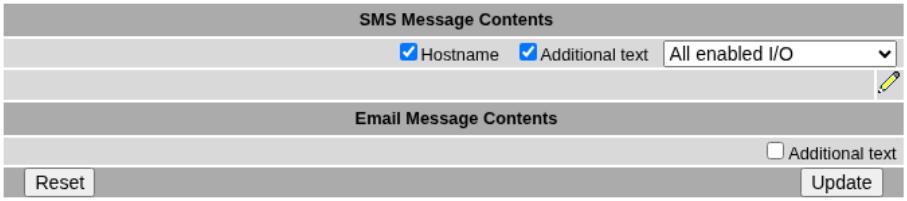


Fig. 5.19: The add additional text to an GPIO message.

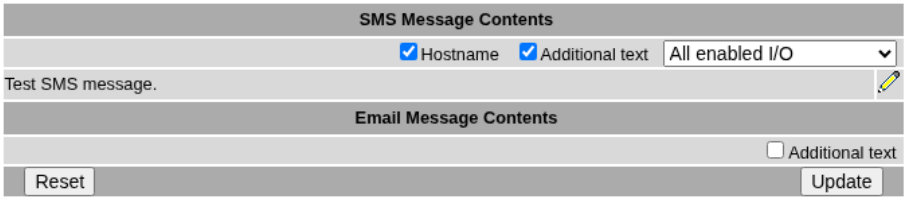


Fig. 5.20: Example of adding additional text to an GPIO SMS message.

Email Message Contents
Should an input or output cause an SMS event to be generated, the values set in these fields determine the contents of the message. The values are:

Additional text
Check to include additional text to be included in the message. When checked a text box will appear containing the additional text to include in the message, as shown in Fig. 5.21. To add or edit text click the  icon beside the text box, an example is shown in Fig. 5.22.

Fig. 5.21: The add additional text to an GPIO message.

5.8 GPIO Example

In this example the two inputs will be enabled and labelled as Door Alarm and Temp Alarm to represent alarm inputs. The host name will be enabled and the Extra text field set to Test site. This configuration is shown in Fig. 5.23.

To enable an SMS and email to be sent on this trigger SMS and email events need to be configured in the management configuration. For details on management refer to the **Management** chapter. Fig. 5.24 shows both Input 1 and Input 2 have been enabled to send an SMS when the alarm contacts are closed.

Fig. 5.22: Example of adding additional text to an GPIO email message.

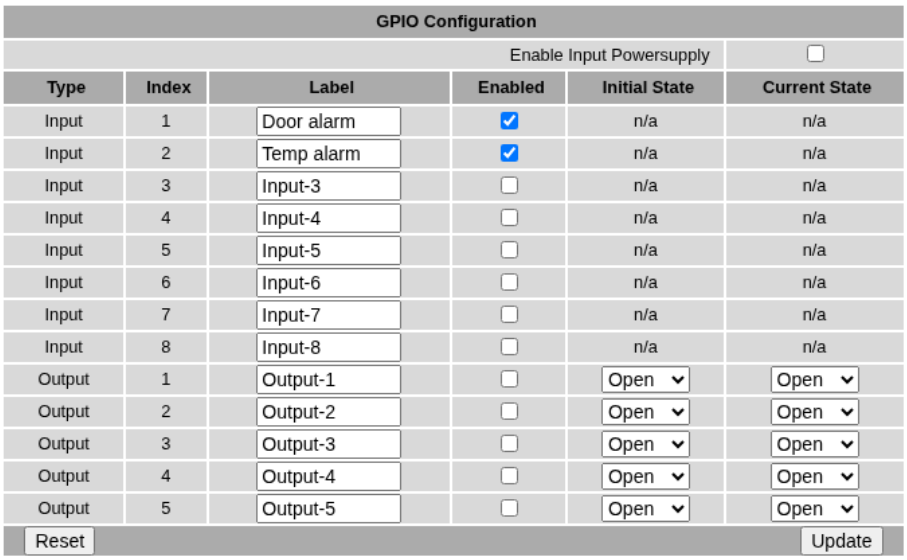
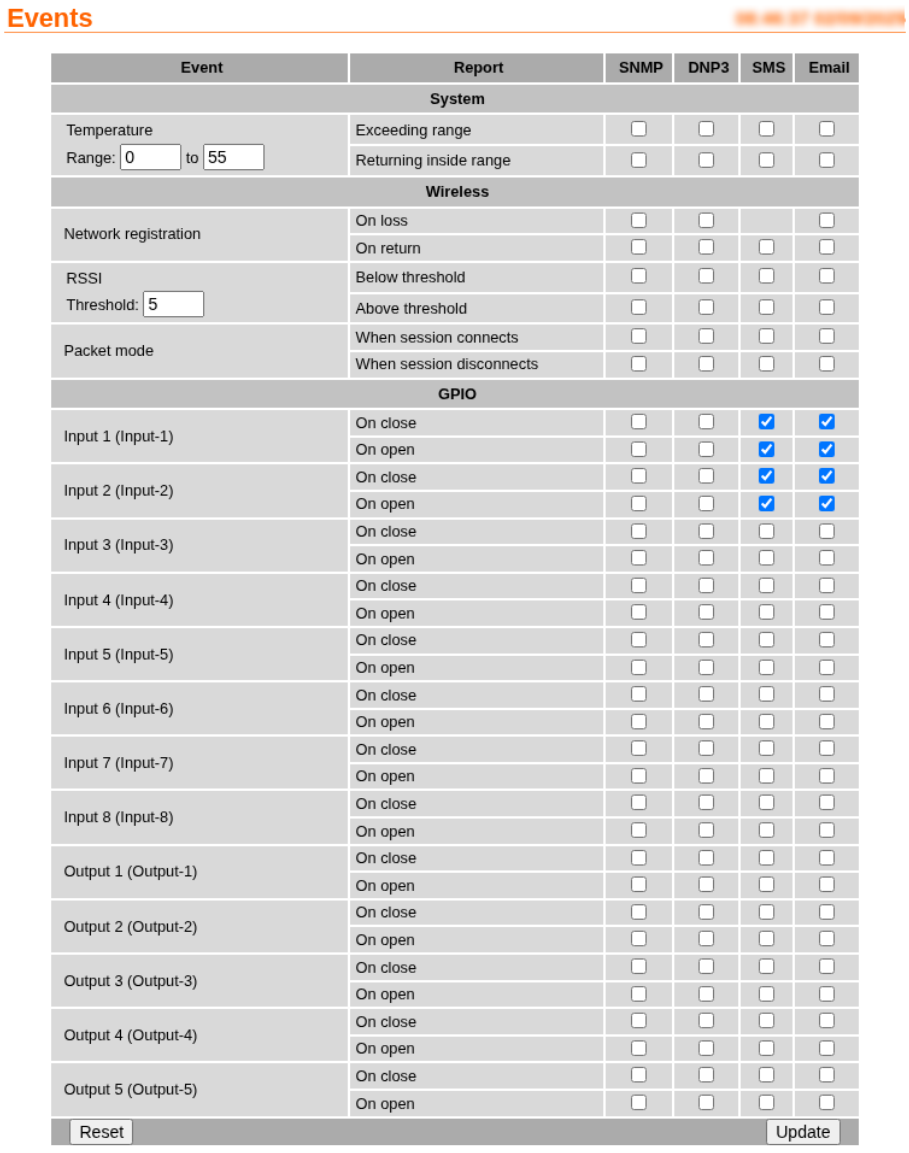


Fig. 5.23: The GPIO configuration example.



Events

Event	Report	SNMP	DNP3	SMS	Email
System					
Temperature Range: 0 to 55	Exceeding range	☐	☐	☐	☐
	Returning inside range	☐	☐	☐	☐
Wireless					
Network registration	On loss	☐	☐		☐
	On return	☐	☐	☐	☐
RSSI Threshold: 5	Below threshold	☐	☐	☐	☐
	Above threshold	☐	☐	☐	☐
Packet mode	When session connects	☐	☐	☐	☐
	When session disconnects	☐	☐	☐	☐
GPIO					
Input 1 (Input-1)	On close	☐	☐	☑	☑
	On open	☐	☐	☑	☑
Input 2 (Input-2)	On close	☐	☐	☑	☑
	On open	☐	☐	☑	☑
Input 3 (Input-3)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 4 (Input-4)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 5 (Input-5)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 6 (Input-6)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 7 (Input-7)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 8 (Input-8)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 1 (Output-1)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 2 (Output-2)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 3 (Output-3)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 4 (Output-4)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 5 (Output-5)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐

Reset Update

Fig. 5.24: The GPIO SMS event configuration example.

If the alarms inputs are now closed the following SMSes end emails will be sent:

First for Input-1 indicating the Door alarm is closed:

SMS

<host>: Test site: Door alarm=closed, Temp alarm=open

The email message contents will be similar to the following:

```
Hostname: <host>
Uptime: 00:21:44
System time: Thur Jun 25 17:21:17 2026
User message:
Test Email message.
Door alarm: Closed
Temp alarm: Open
```

And then for Input-1 indicating the Temp alarm is closed:

SMS

<host>: Test site: Door alarm=open, Temp alarm=closed

The email message contents will be similar to the following:

```
Hostname: <host>
Uptime: 00:23:39
System time: Thur Jun 25 17:23:12 2026
User message:
Test Email message.
Door alarm: Open
Temp alarm: Closed
```

5.9 Location using GNSS

The Location page provides access to the GNSS configuration. The Location page is accessed by selecting the menu *System* → *Location*. A page similar to that in Fig. 5.25 will be shown.

Warning

GNSS functionality requires a GNSS antenna to be connected to the unit. Refer to the GNSS section of the manual for the model being configured for details.

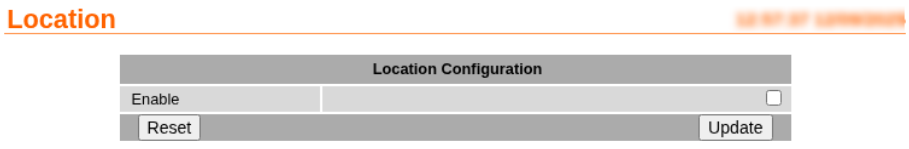


Fig. 5.25: The default Location page.

To enable GPS check the Enable check-box. The page will expand to show the configuration options as shown in Fig. 5.26 on the next page.

Warning

Enabling GPS functionality will increase power consumption. To minimise the power consumption either configure for a manual poll and only update occasionally or set the Periodic fix interval to be a large value.

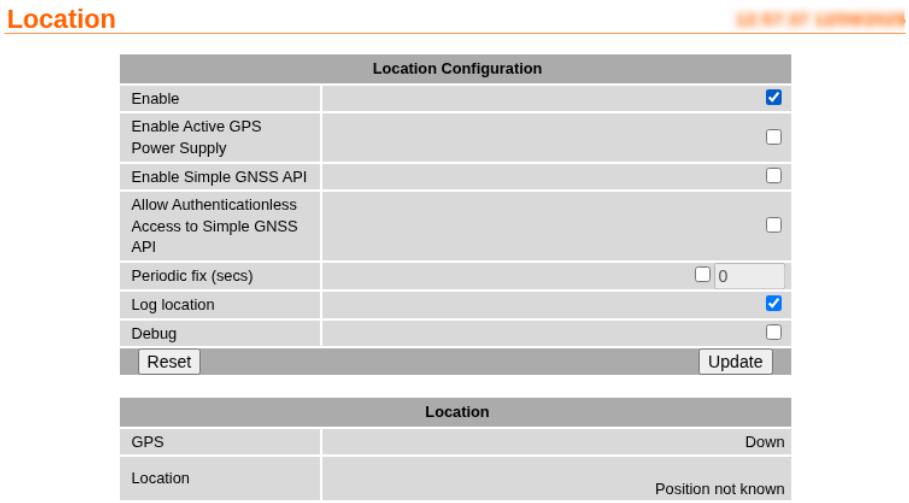


Fig. 5.26: The Location page with GPS enabled.

5.9.1 Location Configuration

Enable
Check to enable GNSS functionality.

Enable Active GPS Power Supply
Enable the active GPS power supply to provide power to the GPS antenna.

Enable Simple GNSS API
Enable a simple GNSS API for basic location data access.

Allow Authenticationless Access to Simple GNSS API
Allow access to the simple GNSS API without authentication.

Periodic fix (secs)
Check to enable periodic GNSS location fixes. If checked the Periodic fix interval field will be enabled. Specify the time interval at which to obtain a GNSS location fix.

Log location
Log the location when a GNSS fix is acquired.

Debug
Enable debugging messages.

Once any changes have been made to the configuration click the Update button the save the changes, only then will GNSS be enabled. A page similar to that shown in Fig. 5.27 will be shown.

5.9.2 Location

GPS
Will report:

Down
When GPS is not Enabled.

Locate Update
When GNSS is enabled.

Location
Will report:

Position not known
While attempting to acquire a GPS fix.

Co-ordinates and Time-stamp
Once a fix has been obtained.

The Locate button will not be displayed until the GNSS settings have been saved by clicking the Update button.

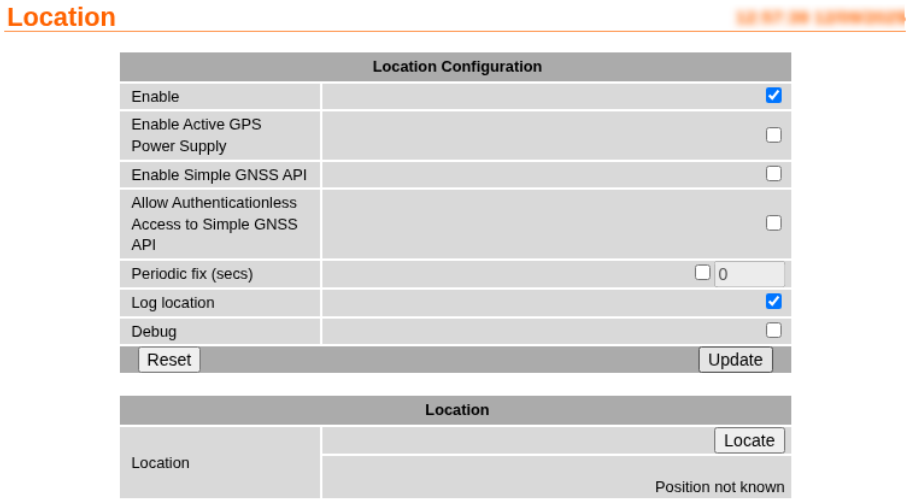


Fig. 5.27: The Location page with GPS configured but no location yet determined.

To obtain a GPS fix click the Locate button. Once the location has been determined it will appear in the location table, as shown in Fig. 5.28.

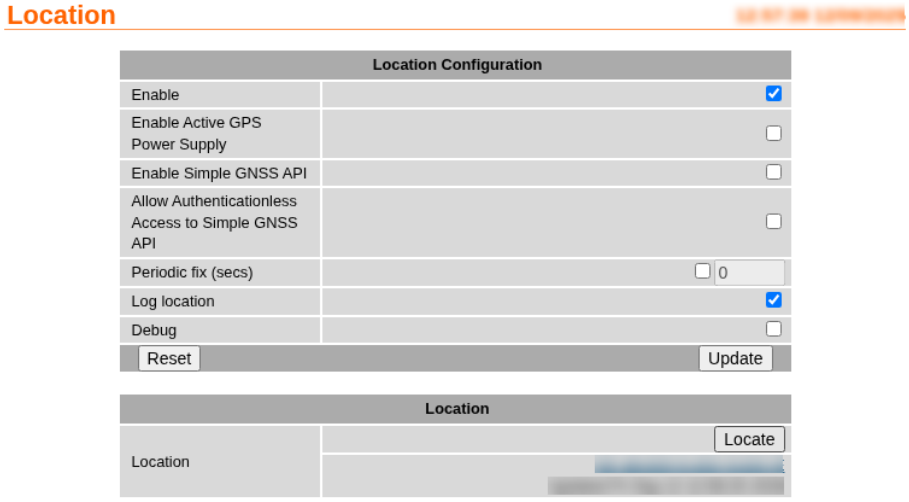


Fig. 5.28: The Location page showing a location.

The location will be written to the log if this option has been enabled.

It will appear similar to that shown:

```
<timestamp>: Location: 33 Degrees 49.147' S 151 Degrees 7.470' E
<timestamp>: Location: 33 Degrees 49.147' S 151 Degrees 7.470' E
```

Where:

<timestamp>: Is the timestamp in the form dd/mm/yyyy hh:mm:ss timezone.

5.10 Support

The Support page provides access to technical support tools and diagnostic information. The Support page is accessed by selecting the menu *System* → *Support*. A page similar to that shown in Fig. 5.29 will be displayed.

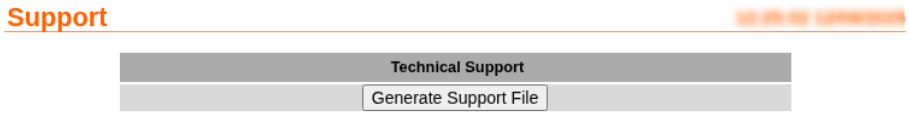


Fig. 5.29: The Support page.

5.10.1 Generating a Support File

The support file contains diagnostic information about the unit's current configuration and operational status. This file can be provided to technical support personnel to assist with troubleshooting and problem resolution.

To generate a support file, click the Generate Support File button in the Technical Support section. Once generated a link to download the file will be provided. The file can then be saved to local storage and forwarded to technical support personnel as required.

5.11 Certificates

The Certificates page provides access to certificate management tools for securing web interface communications. The Certificates page is accessed by selecting the menu *System* → *Certificates*. A page similar to that shown in Fig. 5.30 will be displayed.

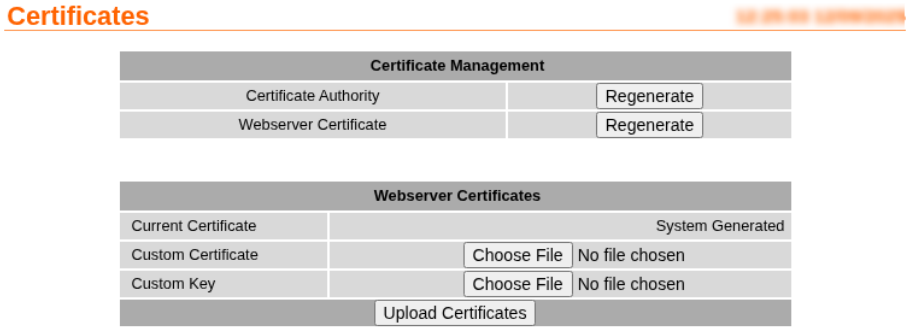


Fig. 5.30: The Certificates page.

5.11.1 Certificate Management

The Certificate Management section provides options to regenerate the internal certificates used by the system.

Certificate Authority

Click the Regenerate button to regenerate the Certificate Authority (CA) certificate. This certificate is used to sign other certificates within the system.

Webserver Certificate

Click the Regenerate button to regenerate the webserver certificate used for HTTPS connections to the web interface.

5.11.2 Webserver Certificates

The Webserver Certificates section allows you to manage custom SSL/TLS certificates for the web interface.

Current Certificate

Shows the currently active certificate type. This will display either "System Generated" for the default self-signed certificate, or "Custom" if a custom certificate has been uploaded.

Custom Certificate

Click Choose File to select a custom SSL certificate file (.crt or .pem format) to upload for use with the web interface.

Custom Key

Click Choose File to select the corresponding private key file (.key format) for the custom certificate.

Upload Certificates

Click the Upload Certificates button to apply the selected custom certificate and key files to the web interface.

> **Warning**
>
> When uploading a custom certificate, ensure that the certificate and key files are correctly matched and valid. An invalid certificate or key may cause the web interface to become inaccessible over HTTPS until a valid certificate is uploaded or the system-generated certificate is restored.

CHAPTER

SIX

WIRELESS

This section describes the GSM / 3G / 4G / 5G Wireless interface configuration options and settings.The two modes of operation that are supported are packet mode and Circuit Switched Data (CSD) mode. CSD mode is only relevant for supported hardware. The configuration settings for each will be described.

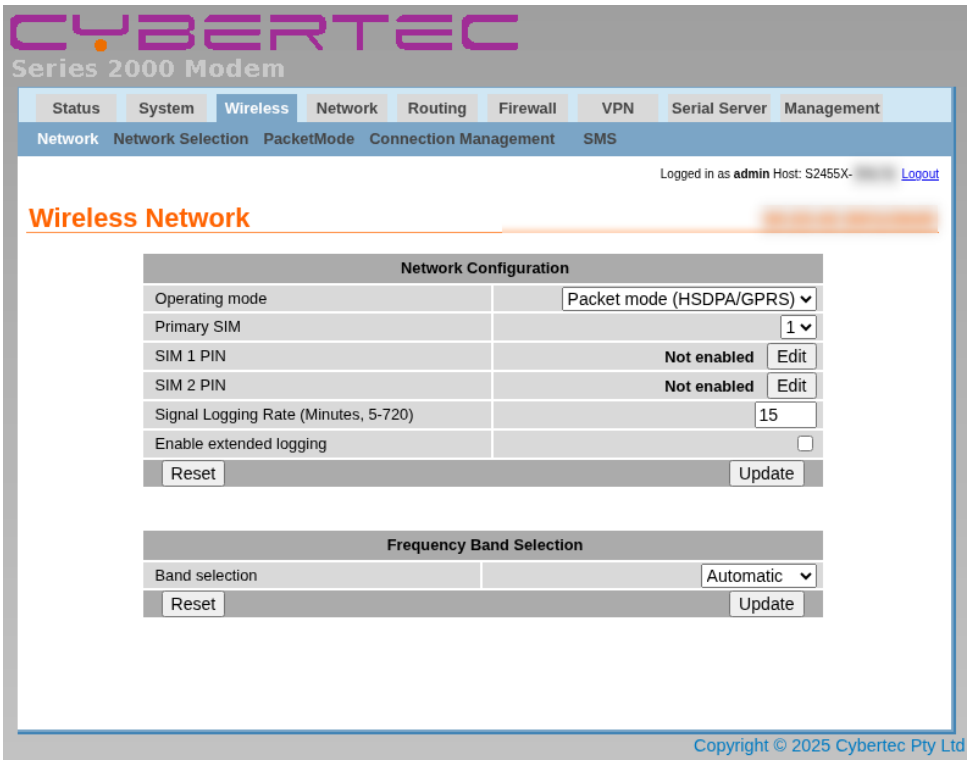


Fig. 6.1: Main Wireless page.

The subsections of the configuration are:

- **Network - Configure the mode of operation, selecting the frequency band** of operation and setting the SIM PIN.
- Network Selection - Configure roaming and network selection criteria
- Packet mode - Configuration of the packet mode settings.
- **Circuit switched mode - Configuration of the circuit switched data mode** settings.
- **Connection Management - Configure the connection management, configure** network and packet timeouts and remote pollers.
- SMS - Configure the Short Message Service (SMS) options and settings.

The Wireless configuration page is accessed by selecting the **Wireless** tab from the main menu. When selected, the page similar to that shown in Fig. 6.1 will be displayed.

6.1 Wireless Network

The Wireless Network options are used to set the operating mode, select the frequency band of operation and set the SIM PIN. To display the Wireless Network page select *Wireless* → *Network* from the menu. The page shown will differ slightly between models, most models will look the same except when it comes to Specify Band selection options and when the number of SIMs differs. Fig. 6.9 shows an example of the wireless network page with the Specify Band option.

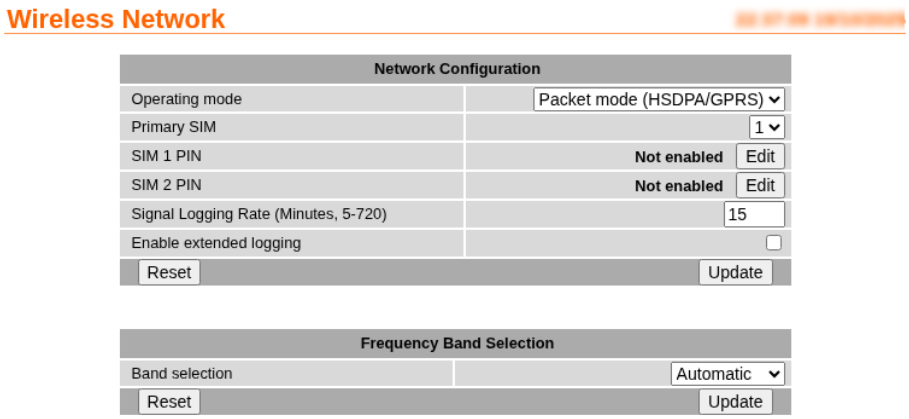


Fig. 6.2: Wireless Network configuration with Automatic option.

6.1.1 Network Configuration

The configuration options for the network configuration are the following:

Operating mode

Set the operating mode of the wireless interface. Three modes of operation are supported for the wireless interface, the options are:

Disabled

The wireless interface is shut-down. No data connections are possible over the wireless interface, this includes SMS.

Packet mode (HSDPA/GPRS)

In packet mode the unit acts as a TCP/IP modem and router, this is the standard and recommended mode of operation. The majority of the functions and services will only be available when operating in this mode. The modem connects to the provider's network and is allocated an IP address. Data can be routed between the LAN ports and the Wireless port. The Serial Server is used to transport serial data over the packet interface.

Circuit switched mode

Circuit Switched Data mode is similar to a traditional dial-up modem. It is mainly intended for the transport of serial data. Connections are established by dialling into the modem using a PSTN modem or dialling out a call via AT commands on the serial port.

> **Warning**
>
> CSD mode is generally no longer supported by network operators and the functionality will be removed in a future firmware version.

Primary SIM
Use to select the primary SIM on models which have the option of installing more than one SIM. The SIM selected will be the first used when attempting to establish a network connection.

SIM n PIN
Indicates if a PIN has been set for the relevant SIM. Click Edit to set the pin, details are shown in the following section. On models with the option of installing more than one SIM a line for each SIM will be present, the PIN for each SIM will need to be set.

Signal Logging Rate (Minutes, 5-720)
The rate, in minutes, at which to output the signal values to the log.

Enable extended logging
Check to enable extended logging for the wireless interface. This option is useful if connection problems are encountered.

Click the Update button to save and commit changes.

6.1.2 Setting the SIM card PIN

The SIM card may have a PIN associated with it. If PIN checking is enabled on the SIM then in order to access the SIM, the PIN will need to be set. To set the SIM PIN click the Edit button in the **SIM PIN** row for the relevant SIM. A dialogue box as shown in Fig. 6.3 will be displayed.

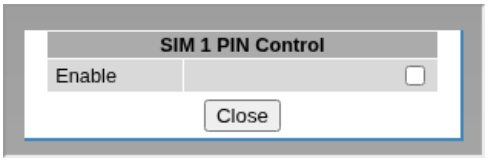


Fig. 6.3: Add SIM PIN dialogue

By default the PIN is not enabled, to enable it check the check-box. The dialogue box change to include additional fields as shown in Fig. 6.4.

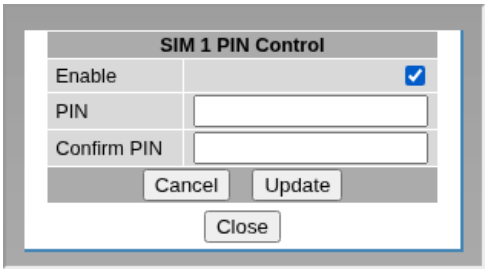


Fig. 6.4: SIM PIN Enabled.

Enter the PIN into both the PIN and Confirm PIN text boxes as shown in Fig. 6.5, the PIN digits will not be shown. The presence of a digit will be indicated by a '•'

Click the Update button to save and commit changes.

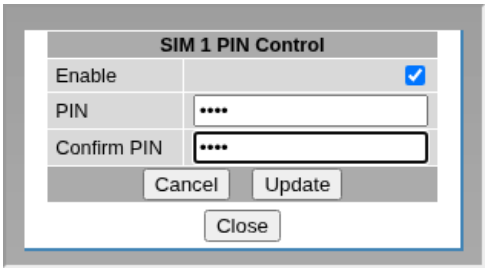


Fig. 6.5: Entering the SIM PIN.

Tip

The PIN will only be saved if the two PINs entered match. If the PINs entered do not match an error will be indicated.

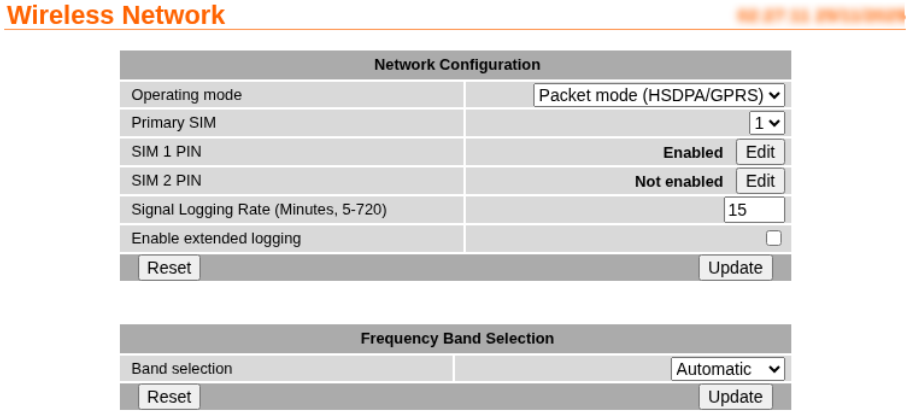


Fig. 6.6: Wireless Network with SIM 1 PIN Enabled.

To change or delete a PIN click the Edit button, a dialogue box as shown in Fig. 6.7 will be shown. To disable the PIN un-check the Enable check-box, edit the PIN click the icon and to delete the PIN click the icon.

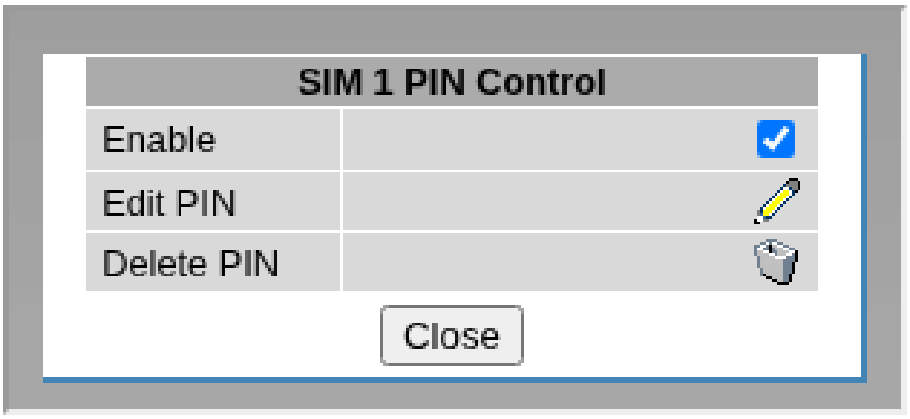


Fig. 6.7: SIM PIN edit dialogue

Tip

Disabling the PIN will not delete it, it can be re-enabled at a later time without re-entering the PIN. To disable

and remove the PIN click the  icon.

6.1.3 Selecting the operating frequency bands

Depending on the model the unit is capable of operating on several frequency bands across NR (5G), LTE (4G), UMTS (3G) and GSM.

> **Tip**
>
> The band selection is slightly different for NR, LTE and UMTS models. Some models allow each individual band to be selected, other models only allow bands to be selected in groups. The settings for each type are provided.

The default setting is Automatic which means all supported frequency bands and technologies are enabled. When the wireless interface is powered on, the unit will start to search for available networks. In general units will connect to the best network technology seen, although big differences in signal strength can cause this to not occur.

In some cases, it may be desirable to limit the frequency bands that are searched. For example, if the network provider only has an 850Mhz UMTS network then the time to register and connect will be reduced if this is the only band searched.

> **Tip**
>
> The default setting of Automatic is the best for most applications. It allows for fall-back options should the main network be unavailable.

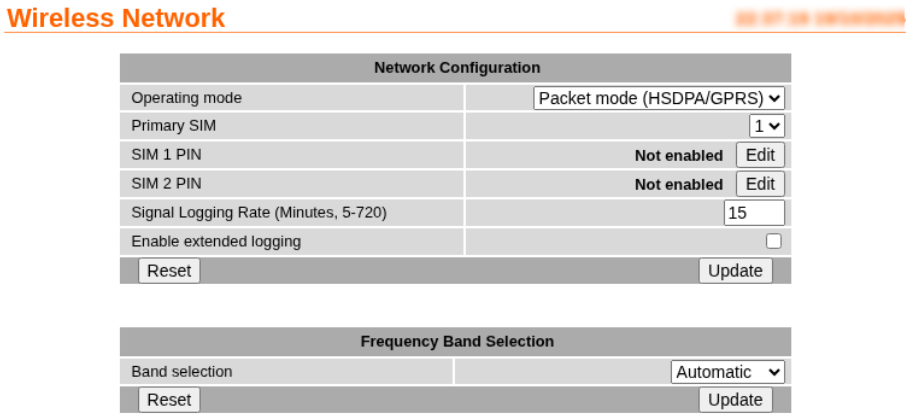


Fig. 6.8: Frequency Band Selection - LTE models.

The following band selection options are available:

Automatic
: Search all supported frequency bands. This is the default and recommended setting.

GSM Only
: Lock to GSM and search all supported GSM bands.

UMTS Only
: Lock to UMTS (3G) and search all supported UMTS bands.

LTE Only
: Lock to LTE (4G) and search all supported LTE bands.

NR Only
Lock to NR (5G) and search all supported NR bands.

Specify
Select specific supported frequencies across from NR, LTE, UMTS and GSM.

LTE Models
When specify is selected individual LTE, UMTS and GSM bands can be select by checking the check-box associated with the desired band. An example is shown in Fig. 6.9.

UMTS Models
When specify is selected bands can be selected in groups:

GSM Selection
Check the check-box to enable and select the desired band group from the drop-down box.

UMTS Selection
Check the check-box to enable and select the desired band from the drop-down box.

Once changes have been made to the frequency bands click the Update button to save and commit changes or click the Update button to cancel any changes and return to the previous settings.

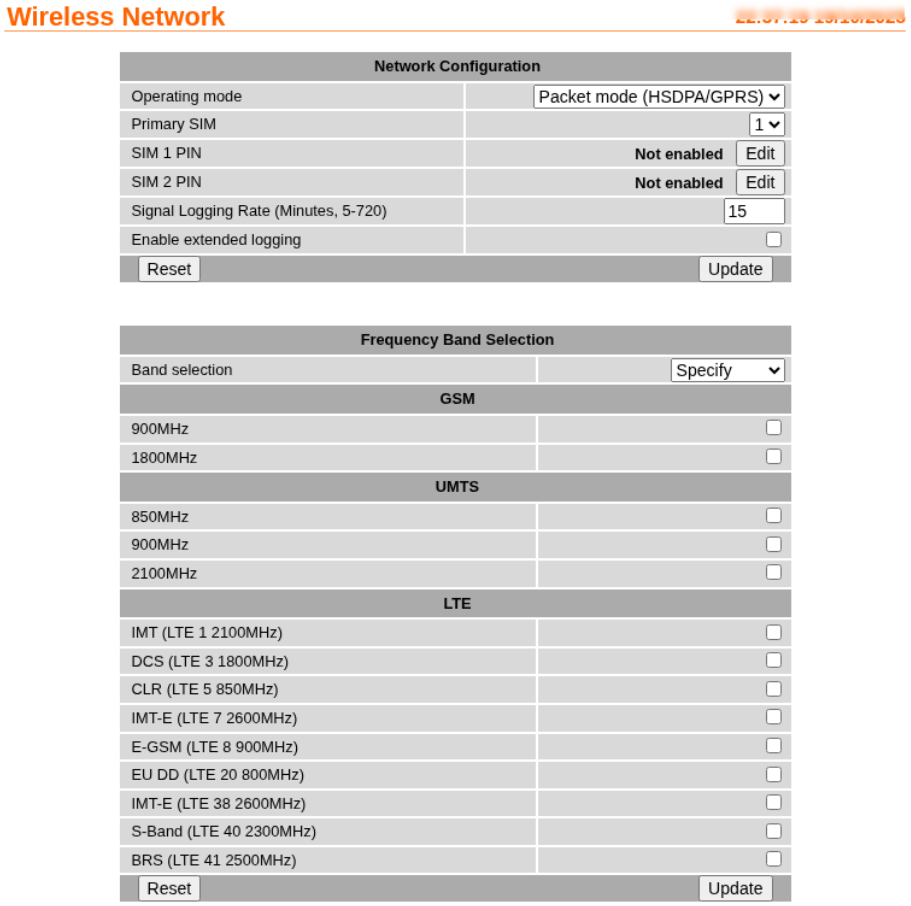


Fig. 6.9: Specifying frequency bands.

Warning

Care should be taken when changing the frequency bands as doing so will initiate a re-start of the wireless interface. This means that any current wireless connection will be disconnected and then the wireless connection

will be re-established. This could result in interruption of data flow. In particular care should be taken when changing the band selection over the wireless interface as this will result in a disconnection from the device.

6.2 Network Selection

Network selection allows for a wireless modem to roam and configure criteria for which networks to connect on. This can be configured per sim slot, allowing for different criteria to be configured on a secondary SIM (on applicable models).

To access the Network Selection page select *Wireless* → *Network Selection*. The screen shown in Fig. 6.10 will be displayed.

Fig. 6.10: Wireless Network Selection

6.2.1 Roaming Settings

The roaming settings allow for the configuration of how the device roams and selects networks. The settings are per SIM slot.

Roaming Mode SIM n
Set the roaming mode for specified SIM n.

Disable
Disable the ability to roam.

Allow
Allow the device to roam. This will happen automatically and will not trigger a scan of available

networks.

Network with Best RSSI
Scan all available networks and connect to the one with the best RSSI, taking technology weightings into account.

First network meeting minimum RSSI
Scan all available networks and connect to the first one that meets the minimum RSSI level.

Preferred PLMN
Scan all available networks and connect based off of the priority order of the configured preferred PLMN list.

The rest of the configuration modes are dependent on which roaming mode is configured. The configuration options will appear/disappear from webpage based off of whether they are suitable for a given roaming mode.

RSSI Minimum Value SIM n
Minimum RSSI value required to connect to a network after a scan. This is valid in the following roaming modes:

- First network meeting minimum RSSI
- Preferred PLMN

Strict Mode SIM n
Don't allow roaming to default networks when no valid networks are found. If enabled and no valid network found, the device will restart the module and rotate the SIM if applicable. This is valid in the following roaming modes:

- Network with Best RSSI
- First network meeting minimum RSSI
- Preferred PLMN

Include internal roaming list SIM n
Parse the internal roaming list and add to allow lists.

This is valid in the following roaming modes:

- Network with Best RSSI
- First network meeting minimum RSSI

Timed Retrigger (Hours) SIM n
Trigger a network scan every x hours. This is valid in the following roaming modes:

- Network with Best RSSI
- First network meeting minimum RSSI

6.2.2 Accessible Networks

This is a list of networks that the most recent scan found. The PLMN, name, technology will all be present and the signal will be reported if a value could be read from the network.

Force Scan
Click to trigger a network scan. Depending on the roaming mode configured for the current active SIM, this may result in a particular network being selected after the scan.

6.2.3 Networks to ignore SIM n

A list of networks that should be ignored when scanning for networks. This list is relevant for roaming modes:

- Network with Best RSSI
- First network meeting minimum RSSI
- Preferred PLMN

To add a network to the ignore list, click on the Add new ignore rule button. You will be taken to a new screen where you can input the details of the network to ignore. Fig. 6.11 shows the page of adding a new ignore rule.

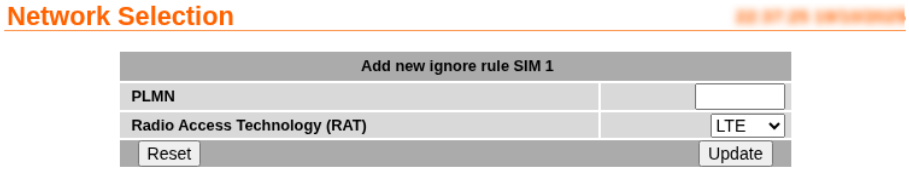


Fig. 6.11: Adding a new ignore rule.

The options are:

PLMN
The PLMN of the network to ignore.

Technology
The technology of the network to ignore.

Click the Update button to save and commit changes.

> **Note**
>
> The order of the ignore rules does not matter.

6.2.4 Preferred Networks SIM n

This list is only relevant if the roaming mode is configured to Preferred PLMN. This list defines the priority order to connect to networks that are found during a scan. There are two ways to configure the list. The first way is to upload a csv file containing the list of preferred networks. The second way is to add networks manually through the web interface.

On uploading a csv file, the existing list will be replaced with the contents of the file. The format of the csv file is:

```
PLMN,Technology
```

Where PLMN is the PLMN of the network and Technology is one of:

- GSM
- UMTS
- LTE
- NR

For example:

```
101,LTE
102,UMTS
```

> **Note**
>
> The order of the entries in the csv file is important as this defines the priority order. Case does not matter.

Besides uploading a csv file, networks can be added manually by clicking the Add new preferred PLMN button. This will take you to a new page where the details of the network can be entered. Fig. 6.12 shows the page of adding a new preferred network.

The options are:

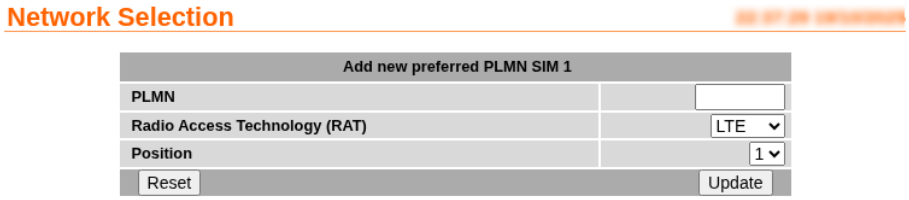


Fig. 6.12: Adding a new preferred network.

PLMN
The PLMN of the preferred network.

Technology
The technology of the preferred network.

Position
The position in the priority order of the preferred network. 1 is the highest priority.

Click the Update button to save and commit changes. The new entry will be added to the end of the list. The entries can be edited or deleted later.

6.3 Packet Mode Configuration

Before the modem can establish a packet connection, the details of the connection must be set up in a connection profile. Some networks will also require the packet connection details to be configured before a network connection can be established. This section details the process of adding, editing and deleting a connection profile. While most configurations will only need one configuration profile, multiple profiles are supported. This is particularly helpful in modems that support multi SIM, as it allows for different profiles to be configured for each SIM.

To access the packet mode configuration, select *Wireless* → *PacketMode* from the menu. The screen shown in Fig. 6.13 will be displayed.

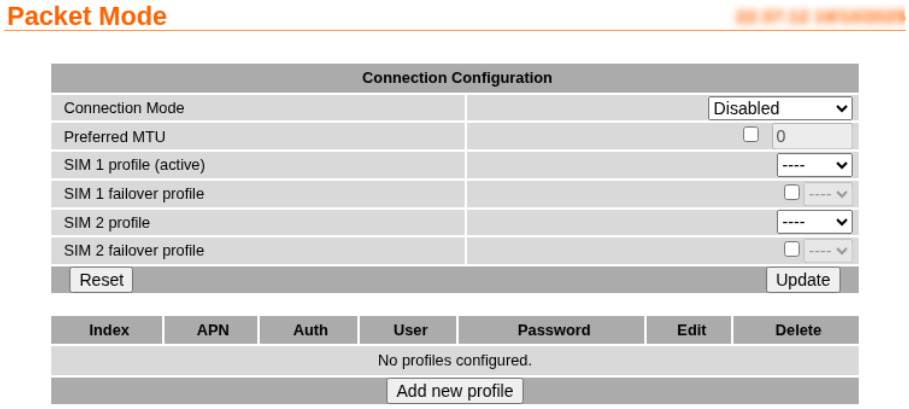


Fig. 6.13: Wireless Interface Packet mode settings

6.3.1 Connection Configuration

By default packet mode is disabled and no profiles are configured.

Connection Mode

Disabled
Packet connections are disabled.

Always Connect
Establish and maintain a packet connection.

Automatic
Establish a connection only when VRRP master. In order for this to function VRRP must also be configured, for details refer to section VRRP of chapter Routing.

Preferred MTU
When enabled, the preferred MTU is set on the wireless interface. Depending on the network and the model types interaction with the network, this value may be effective or ignored. When disabled, the default MTU value will depend on the model and network.

SIM n profile
Select the profile for the corresponding SIM.

The options are:

Index
Select the index of a defined profile. Refer to next section on how to add connection profiles.

Via AT
This option is only available on models that have serial ports. The unit is configured to operate in modem emulation mode and the profile details will be provide via an AT command. Refer to the Serial Server section for details on configuring Modem Emulation.

SIM n failover profile
Select the failover profile for the corresponding SIM. This profile will be used if the primary profile fails to connect.

The options are:

Index
Select the index of a defined profile. Refer to next section on how to add connection profiles.

Click the Update button to save and commit changes.

6.3.2 Adding Connection Profiles

To add a new profile, click the Add new profile button, the add entry page will display as shown in Fig. 6.14.

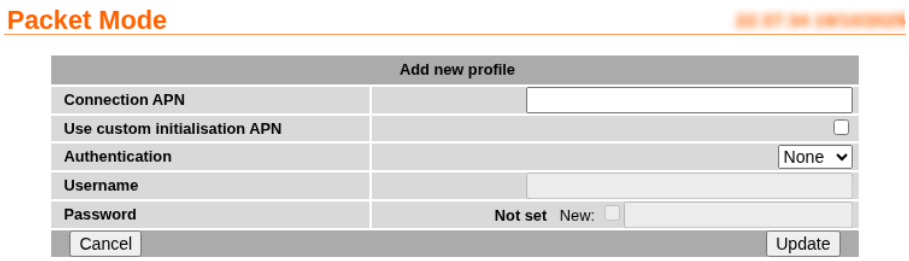


Fig. 6.14: Adding a new profile

The settings required are listed below:

APN
This is the name of the network provider's Access Point Name (APN).

Use custom initialisation APN
When enabled, a config option will appear to define an **Initial APN**. The Connection APN will be used as the initialisation APN if this is not set.

Initial APN
Define an initial APN (also known as a bearer) to be used as an alternative to the connection APN.

Authentication
For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None
No authentication is performed.

PAP
The Password Authentication Protocol is used.

CHAP
The Challenge-Handshake Authentication Protocol is used.

Username
For connections with **PAP** or **CHAP** selected for authentication, this is the user-name the modem will use to authenticate.

Password
For connections with **PAP** or **CHAP** selected for authentication, this is the password the modem will use to authenticate. In order to set a password click the check box marked **New** then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

Tip

The network provider will specify the required settings for completing a connection profile. The provider may not supply a user-name and password if network authentication is not required. In this case set the **Authentication** to **None**. The only required field is the APN.

Once the profile has been entered click the Update button to save and commit changes.

6.3.3 Example of Adding a Connection Profile

In this example a profile will be added with the following details:

APN
apn_string

Use custom initialisation APN
Disabled

Authentication
CHAP

Username
username

Password
password

To add a new profile, click the Add new profile button, the add entry page will be displayed, add the details as shown in Fig. 6.15

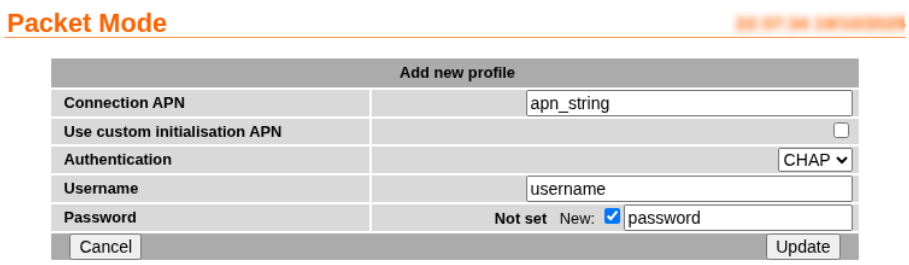


Fig. 6.15: Profile added and selected

Click the Update button to save and commit changes.

The page will revert to the standard packet mode page and the profile will be listed in the profiles table as shown in Fig. 6.16.

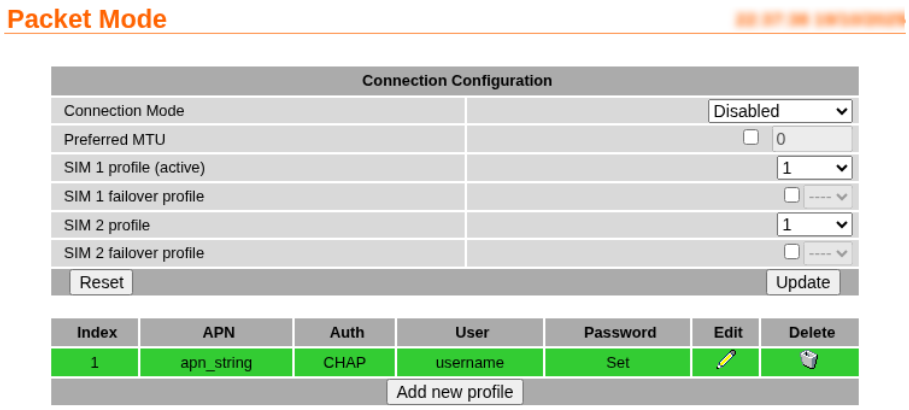


Fig. 6.16: Profile added and selected

> **Tip**
>
> As no profiles were previously selected the new profile will automatically be associated with all available SIMs. If more profiles are added the SIM index can be changed.

6.3.4 Enabling a wireless connection

To complete the configuration of the wireless connection, the connection needs to be enabled. This is done by setting the **Connection Mode**. The connection options available are:

Connection Mode

Disabled
: Packet connections are disabled.

Always Connect
: Establish and maintain a packet connection.

Automatic
: Establish a connection as required.

Always Connect is generally the best option.

Once the setting has been selected click the Update button to save the change to the connection state. Once the state has been set, the modem will attempt to establish a connection.

Fig. 6.17 shows an example of a completed packet mode configuration.

6.3.5 Adding Further Profiles

Additional profiles may be added by following the same process as above. Fig. 6.18 and Fig. 6.19 show the result of adding a second profile. Notice that the profile with Index 1 is highlighted green as it is the currently selected profile.

To change the selected profile select the required index number from the Current profile drop down box in the Connection Configuration section and click Update. The page will update and the selected index will now be highlighted. Fig. 6.20 is an example with the second profile added above selected.

> **Tip**

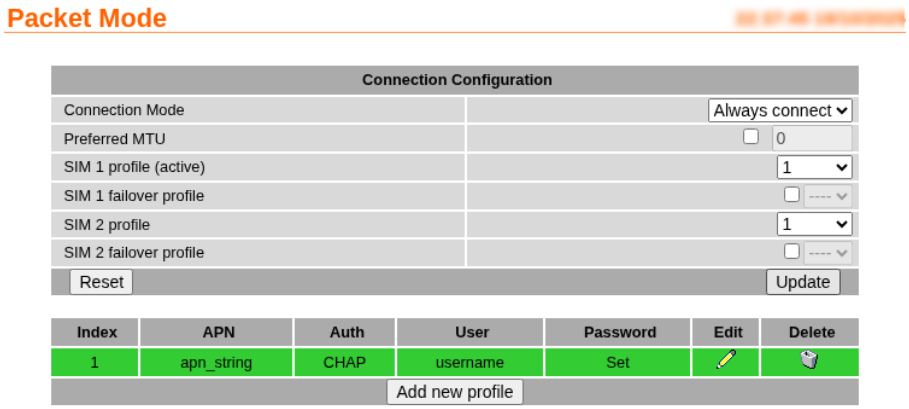


Fig. 6.17: Completed wireless configuration

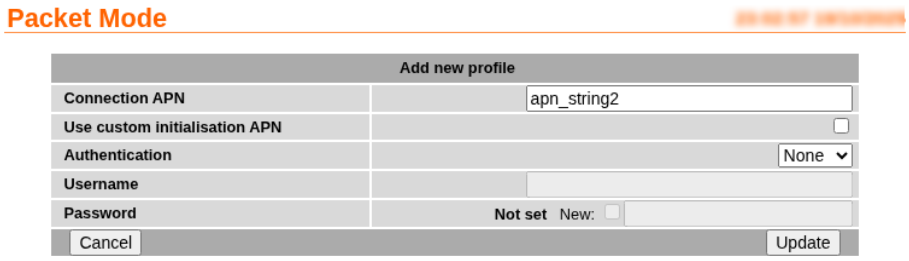


Fig. 6.18: Adding a second profile.

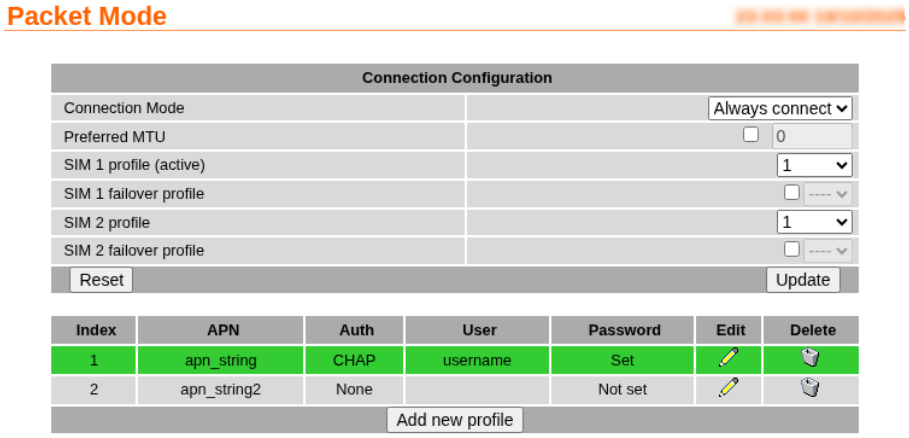


Fig. 6.19: List of profiles now listing 2 profiles.

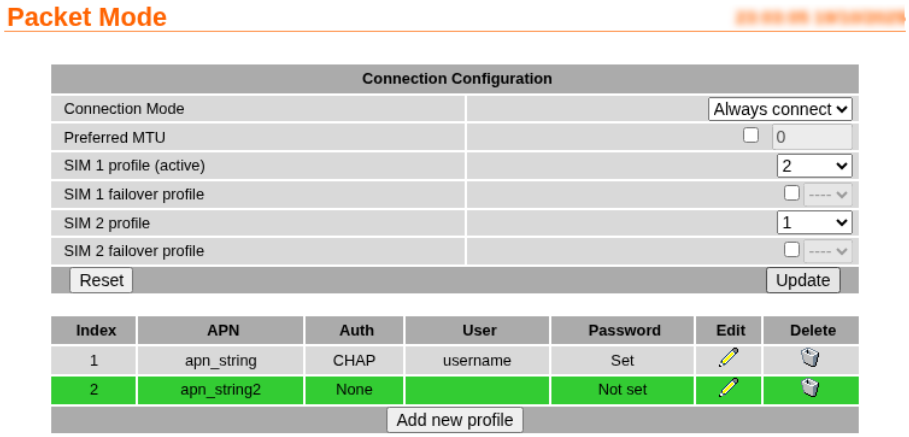


Fig. 6.20: Second profile selected.

For models with more than one SIM the highlighted profile will be for the Active SIM. In the example shown in Fig. 6.20 the Active SIM is SIM 1 and the selected profile for SIM 1 is Index 2 so the profile with Index 2 is highlighted.

6.3.6 Editing a profile

To edit an existing profile click on the  icon located in the **Edit** column for the profile to be edited. Complete the changes to the profile then click **Update** to commit the changes. Fig. 6.21 illustrates editing of the second profile, in this example the authentication is changed from None to PAP and a Username and Password are added. The updated profile list is shown in Fig. 6.22.

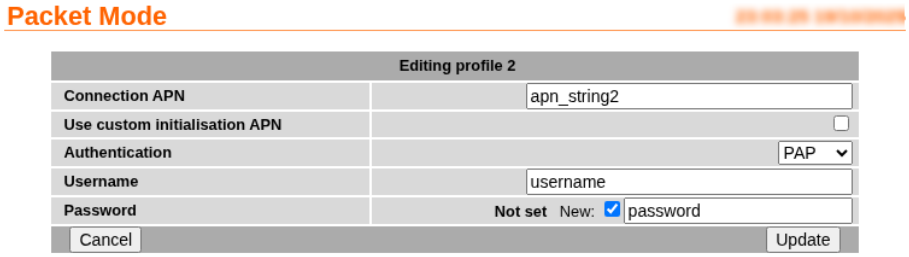


Fig. 6.21: Editing the second profile.

6.3.7 Deleting a profile

A profile can be deleted by clicking the  icon located in the **Delete** column for the profile to be deleted. Click **OK** to confirm the deletion. Fig. 6.23 shows the process of deleting a profile. In this example the second profile has been deleted.

After clicking OK the updated profile list appears as shown in Fig. 6.24

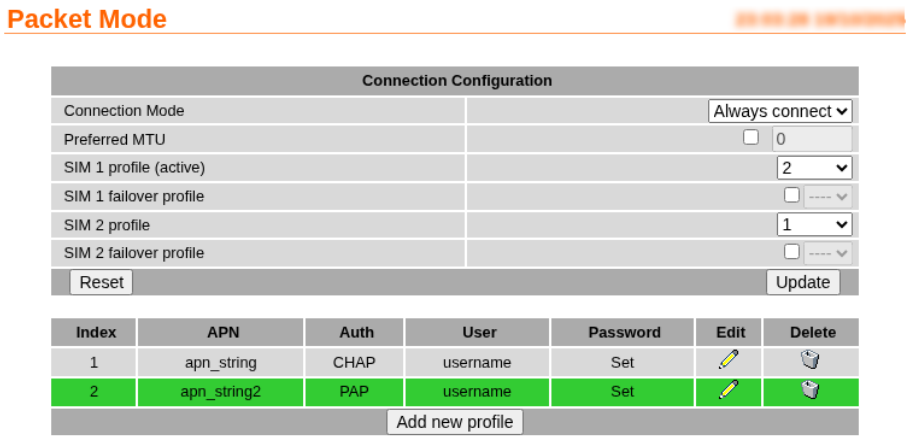


Fig. 6.22: Profile list after editing the second profile.

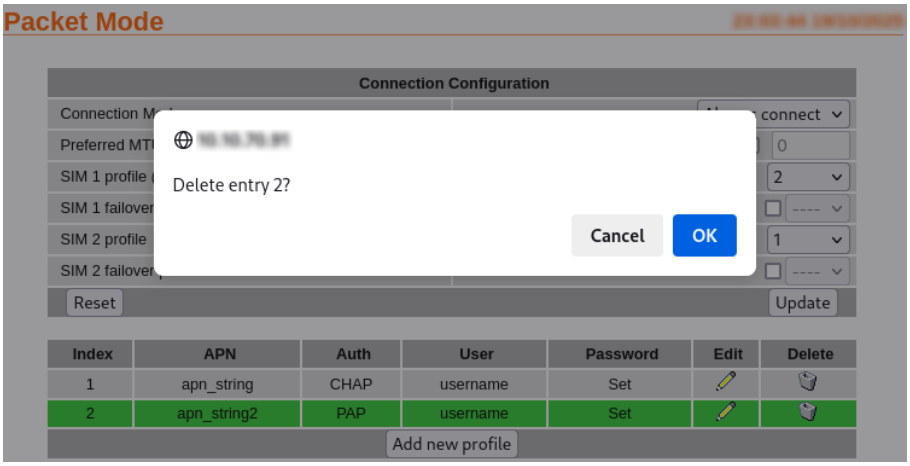


Fig. 6.23: Deleting the second profile.

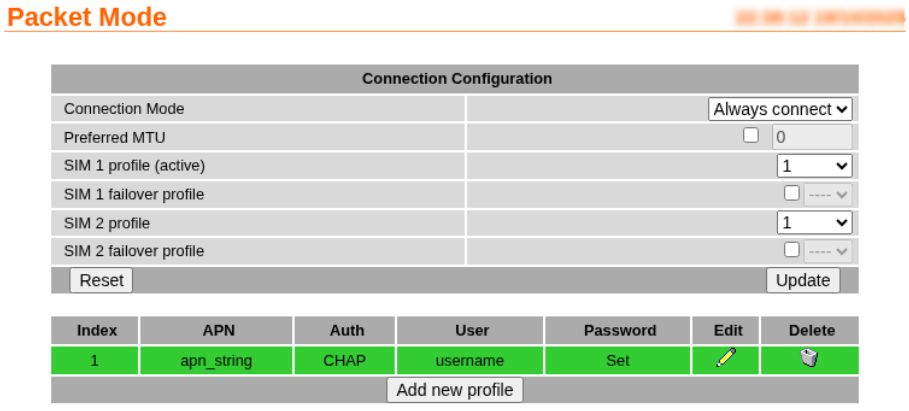


Fig. 6.24: Profile list after deleting the second profile.

> **Tip**
>
> As the selected profile for SIM 1 was deleted, the index was automatically set to index 1. This is because a valid profile will always be associated with a SIM where possible.

6.3.8 Checking the status of the connection

To check the status of the connection select **Status** from the main menu and **Wireless** from the sub-menu. The wireless status page will be displayed which will look similar to that shown in Fig. 6.25. The status of the connection will change as the modem connects to the network. The status will change through *Checking, Connecting* and finally *Connected* as a connection is established. To see the value changing the page will need to be refreshed.

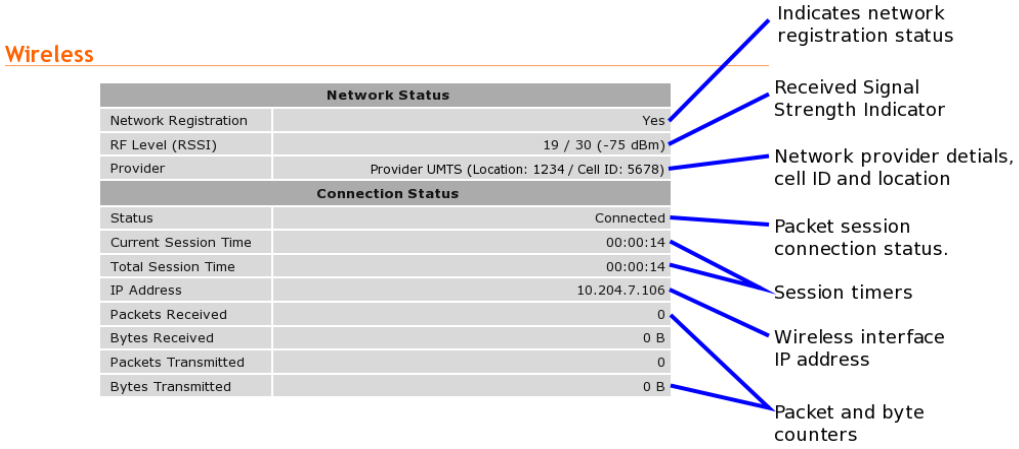


Fig. 6.25: Wireless Status page

The section titled **Network Status** details the quality of the service available from the wireless network.

SIM Card

This field will only be shown if an error with the SIM card has been detected, and will be reported as **Absent or faulty** or **PIN needed** as shown highlighted in Fig. 6.26 and Fig. 6.27.

If the SIM card fault is reported, possible causes include:

- The SIM card has not been inserted correctly. Refer to the manual for the model being configured, for details on how to insert the SIM card.
- The SIM card pin number has not been entered or is incorrect. Refer to section *Setting the SIM card PIN* for details on entering the SIM card PIN.

Network Registration

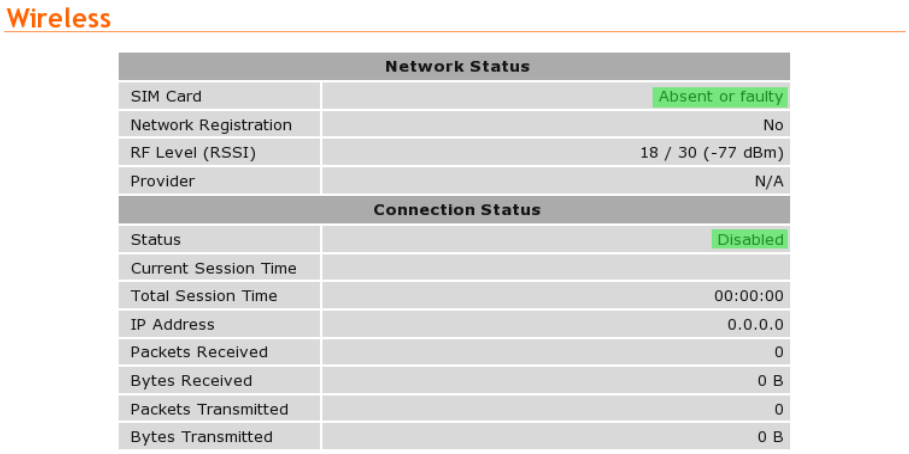
This field indicates if actively registered to the wireless network. No connection is possible without registration.

If the network registration field is indicated as **No**, possible causes include:

- Poor signal strength. Check the antenna is properly connected and experiment with different locations to achieve a higher RF Level.
- Problem with the SIM card. Ensure the SIM card is fitted correctly and is currently enabled with the network provider.
- The SIM card is not correctly enabled with the network provider. Verify with the provider that the SIM is currently active.

RF Level

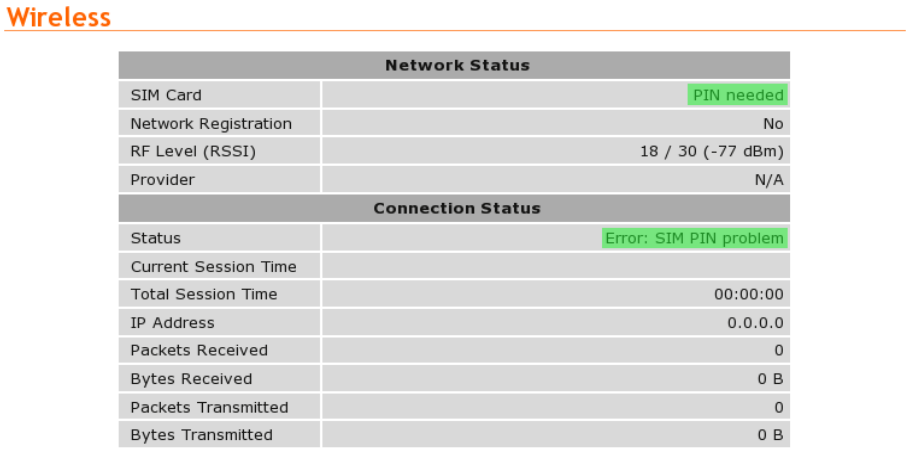
Indicates the current strength of received signal from the network, with a maximum of 30. Any level over 10 should provide acceptable connection speeds.



Wireless

Network Status	
SIM Card	Absent or faulty
Network Registration	No
RF Level (RSSI)	18 / 30 (-77 dBm)
Provider	N/A
Connection Status	
Status	Disabled
Current Session Time	
Total Session Time	00:00:00
IP Address	0.0.0.0
Packets Received	0
Bytes Received	0 B
Packets Transmitted	0
Bytes Transmitted	0 B

Fig. 6.26: Wireless Status page showing a SIM Absent fault.



Wireless

Network Status	
SIM Card	PIN needed
Network Registration	No
RF Level (RSSI)	18 / 30 (-77 dBm)
Provider	N/A
Connection Status	
Status	Error: SIM PIN problem
Current Session Time	
Total Session Time	00:00:00
IP Address	0.0.0.0
Packets Received	0
Bytes Received	0 B
Packets Transmitted	0
Bytes Transmitted	0 B

Fig. 6.27: Wireless Status page showing a SIM PIN required fault.

Connection Status
The section shows the statistics for the current connection.

Status
Indicates the current status of the connection. If the connection is active this will show **Connected** as highlighted in Fig. 6.25. If the connection is not active it will show **Disconnected**.

If **Connected** is not indicated verify that the **Connection state** is **Always connect** in the packet mode configuration.

If the **Status** field always shows **Connecting...**, a problem with the APN, user-name or password is likely. Check these values and settings with the network provider. Refer to section *Connection Configuration* Packet Mode for details on how to enter these values and create a profile.

Session Statistics
The session statistics provide information on the current connection session.

The fields list the length of time connected, IP address allocated by the network and data counters. All of this information will reset if a connection is restarted, except the *Total Session Time* field, which will accumulate across all sessions.

6.4 Connection Management

The purpose of connection management is to create and maintain reliable connections that can detect errors and recover as quickly as possible. The connection management is divided in two areas:

Connection establishment
Determines how the modem manages the establishment of a connection to the network.

Connection maintenance
Determines how the modem manages the connection to the network once established.

To access the connection management options, select *Wireless* → *Connection Management* from the menu. The connection management page as shown in Fig. 6.28 will be displayed.

6.4.1 Connection Establishment

The connection establishment options are used to set the parameters for initial connection to a provider's wireless network. The options are:

Rotate SIM
Check to cycle through to the next available SIM should the connection fail to be established. Option only present on models with more than one SIM.

Secondary SIM hold period (mins)
Check to enable a hold time for the secondary SIM and then specify the number of minutes to hold. If enabled, when the secondary SIM is selected it will stay connected using that SIM for the hold time and then try to establish a connection using the primary SIM. Option only present on models with more than one SIM.

Timeout for network initialisation
Specify the maximum time in seconds to allow for a network initialisation. The minimum value accepted is 60 seconds, the default value is 600 seconds.

Timeout for connection establishment
Specify the maximum time in seconds to allow for a connection to be established. The minimum value accepted is 30 seconds, the default value is 90 seconds.

Poll on connection establishment
Check to enable and specify the poll re-try period, the minimum value is 20 seconds. If enabled a remote poll will be completed before the connection is considered successful. The purpose of this option is to ensure that not only has a network connection been established but also that end-to-end connectivity exists. The modem does this by polling a remote server using ICMP (Ping) or a TCP socket connection. Should the poll fail, the

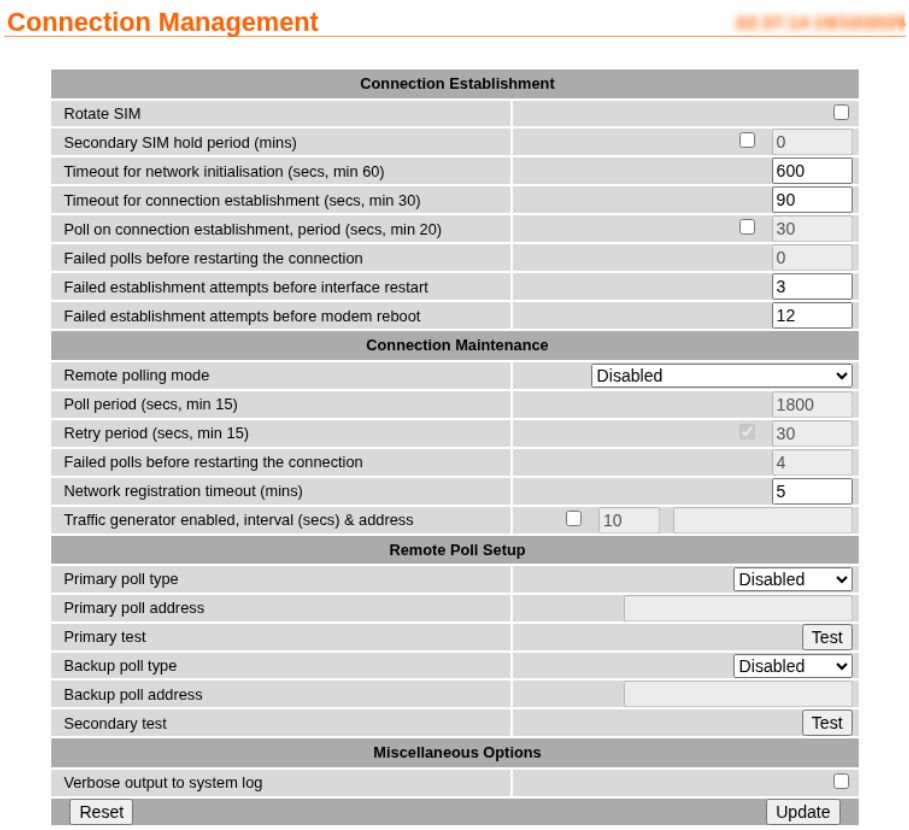


Fig. 6.28: Wireless connection management

modem retries at the specified interval for the number of polls specified in **Failed polls before restarting the connection**. If this option is enabled then the **Remote Poll Setup** must be enabled and configured correctly.

Failed polls before restarting the connection
Set the number of failed polls before the connection is considered to have failed to establish. A value of 0 disables poll on connection establishment. This option is only available when **Poll on connection establishment** enabled.

Failed establishment attempts before interface restart
Specify the number of failed connection attempts before restarting the wireless interface. Set this value to *0* to disable.

Failed establishment attempts before modem reboot
Specify the number of failed connection attempts before re-booting. Set this value to *0* to disable.

Failed establishment attempts before dropping to CSD
Specify the number of failed connection attempts before switching to Circuit Switched Data (CSD) mode. Set this value to *0* to disable the fail-over to CSD feature.

Time to spend in CSD
Specify a time in minutes to remain in CSD mode before reverting to packet mode and attempting to establish a connection. This value is only used if the **Failed establishment attempts before dropping to CSD** option is set to a value greater than *0*.

6.4.2 Connection Maintenance

The connection maintenance refers to the tests employed to determine if a valid network connection is available. Should the connection maintenance test fail then attempts will be made to re-establish the connection.

The following options control connection maintenance:

Remote polling mode
Specify the connection maintenance operating mode. Four modes are supported:

Disabled
Connection maintenance is disabled. (Default)

Poll at fixed interval
Poll the servers specified in the **Remote Poll Setup** at the interval specified.

Poll if Rx idle for interval
Only poll the servers specified in the **Remote Poll Setup** when no data has been received from the wireless interface for the specified interval.

Reconnect if Rx idle for interval
Monitor the receive data and reconnect if no data has been received by the wireless interface for the specified interval. This mode is a good choice for configurations that already employ polling traffic, such as when using the SSL VPN or IPsec VPN with dead peer detection.

Poll period
Specify the time interval in seconds between polls. Minimum value of 15 seconds.

Retry period
Specify the time in seconds to retry the poll after a failed poll. Minimum value of 15 seconds.

Failed polls before restarting connection
Specify the number of failed polls to declare the link failed and to re-start the establishment process.

Network registration timeout
Specify the time in minutes the time-out for network registration attempt after a polling failure.

Traffic generator enabled, interval & address
Check to enable the traffic generator, and specify the time interval between data packets and the address to which to send the packets. The traffic generator is used to generate transmit data, it sends a data packet at the specified interval without expecting a response.

6.4.3 Remote Poll Setup

The remote poll set-up is used to specify the poll type to use and the address of the server to poll. A primary and backup server may be specified. The backup server will be used if the primary server cannot be contacted. The options for each poll are:

Primary Poll type
Specify the poll type. The options are:

Disabled
The poll is disabled.

Ping (ICMP)
Ping the specified address.

TCP Socket
Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Primary Poll address
Specify the address of the primary server to poll. The format used depends on the poll type:

Ping (ICMP)
Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket
Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Primary test
Click the test button to test the poll.

Backup Poll type
Specify the poll type. The options are:

Disabled
The poll is disabled.

Ping (ICMP)
Ping the specified address.

TCP Socket
Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Backup Poll address
Specify the address of the backup server to poll. The format used depends on the poll type:

Ping (ICMP)
Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket
Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Secondary test
Click the test button to test the poll.

6.4.4 Miscellaneous Options

Verbose output to system log
Check to enable sending of verbose connection information to the system log. As the size of the system log is limited, this option should only be enabled if connection problems are experienced.

Click the Update button to save and commit changes.

6.5 Circuit Switched Data (CSD) Mode

Warning

CSD mode is generally no longer supported by network operators and the functionality will be removed in a future firmware version.

Note

In order for Circuit Switched Data mode to work, the following will need to be checked:

- The network operator supports Circuit Switch Data (CSD); and
- The SIM is provisioned for Circuit Switch Data (CSD).

Circuit Switched Data (CSD) mode works in similar manner to a traditional dial-up modem. Connections are established by dialling into the modem or by dialling out to another modem (PSTN or 4G/3G/GSM). Unlike packet mode, where data is carried over in packets over IP networks, circuit switched mode transports serial data through the telephone network. Typically CSD offers much lower data rates than packet mode (CSD rates are around 9600bps).

The configuration for CSD mode is accessed by selecting *Wireless→Circuit Switched Mode*, the main CSD configuration page is shown in Fig. 6.29 and Fig. 6.30.

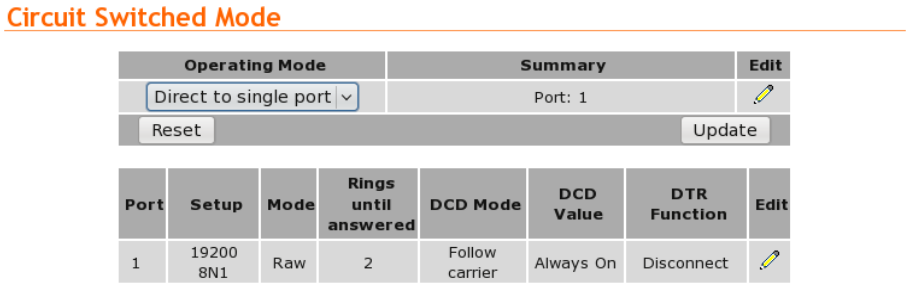


Fig. 6.29: Circuit switched configuration

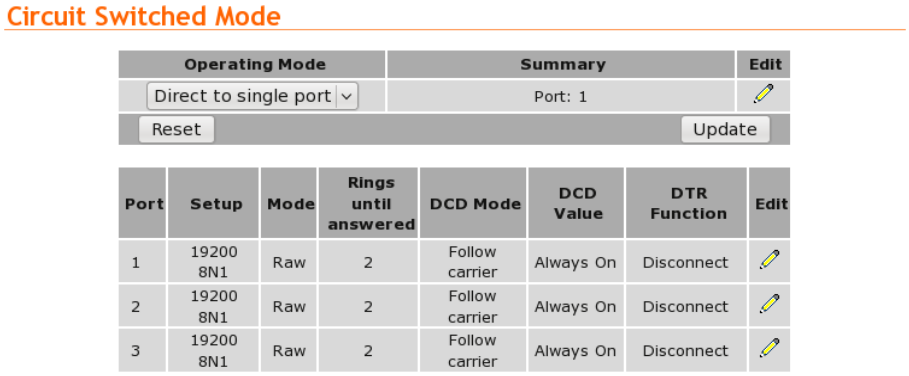


Fig. 6.30: Circuit switched configuration

Note

The number of serial Ports listed is model dependent. Fig. 6.29 shows the Circuit Switch Mode page for a model with 1 serial port while Fig. 6.30 shows the page for a 3 port model.

The Operating mode can be configured for one of four different CSD operating modes:

Direct to single port
: This is the simplest mode and most like a traditional dial-up modem. An AT command interface is provided at a single selected serial port. This port can then be attached to a device (eg. PLC) which expects to be connected to a basic dial-up modem. The device is able to 'dial-out' using standard AT commands. If an incoming call is received, the modem will indicate this to the device which is able to answer the incoming call again using standard AT commands.

Multiplexed mode
: The multiplexed mode allows any one of the available serial ports or the PPP server to be selected at the time of connection. This is achieved through having a virtual console to which the initial connection is made. The caller can then issue a command to select a port. Once selected, all data will be directed to the selected port.

PPP server
: In this mode the unit acts as a PPP remote access server. After dialling in, an IP connection is established between the modem and the calling computer using the Point-to-Point Protocol (PPP). Once the PPP connection has established, all of the packet services of the modem, including the web server and serial server, can be accessed.

PPP dialout
: In this mode the units acts as a PPP client and will connect or dial a remote PPP server. After dialling, an IP connection is established between the modem and the server. Once this connection has been established, all of the packet services of the modem, including the web server and serial server, can be accessed.

6.5.1 Setting serial port parameters

Where the chosen CSD operating mode is **Direct to single port** or **Multiplexed mode**, it will be necessary to configure the parameters of the serial ports to match the devices attached to the modems. This configuration is set in the lower table on the CSD configuration page. To begin editing a port's set-up, click the  icon in the row for that port. The port editing page will display as shown in Fig. 6.31.

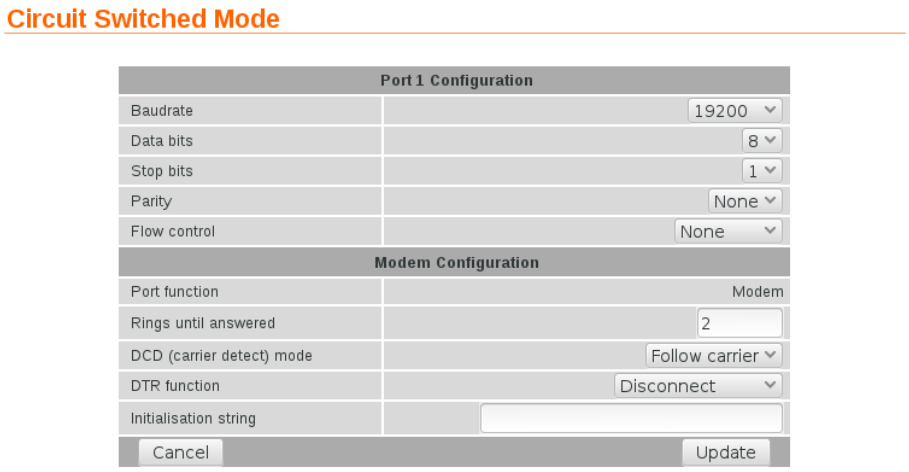


Fig. 6.31: Editing serial port configuration.

For each port, the following parameters can be set:

Port n Configuration Baudrate
The port can be configured for any standard baud rate from 300 baud to 230400 baud.

Data bits
The port can be configured for operation with 5 to 8 data bits.

Stop bits
The port can be configured for operation with 1 or 2 stop bits.

Parity
The port can be configured for none, odd or even parity.

Flow control
The serial server port can be configured for the following modes:

None
No flow control is enabled.

Hardware
The port will use the RTS and CTS handshake lines to control the flow of data.

Software
The port will use XON/XOFF software flow control. The XOFF character is hex 0x11. The XON character is hex 0x13.

Both
The port will use both hardware and software flow control.

Modem Configuration

Port function
When the CSD operating mode is **Multiplexed**, each serial port can be selected to function as follows:

Modem
The modem will generate an AT command interface at the serial port. A device attached to the port can use standard AT commands to dial and receive calls.

Raw
No AT command interface will be generated at the serial port. When the port is selected from the virtual console, a transparent data pipe is created between the serial port and the wireless port.

Rings until answered
For ports configured for **Modem** mode, this field determines the default number of rings the modem will wait before automatically answering a call. This is equivalent to setting the ATS0 S-Register in a conventional modem.

DCD mode
For ports configured for **Modem** mode, this field determines the default state of the Data Carrier Detect (DCD) handshaking line. The following modes are supported:

Always on
Regardless of the online state of the port, the DCD line will be active. This is equivalent to issuing the AT Command: AT&C0.

Follow carrier
The DCD line will be active when the port is in the online state. This is equivalent to issuing the AT Command: AT&C1.

DTR function
For ports configured for **Modem** mode, this field determines the default response of the modem to changes in the Data Terminal Ready (DTR) handshaking line. The following modes are supported:

Ignore
The port will ignore changes to the state of DTR. This is equivalent to issuing the AT Command: AT&D0.

Command mode
If the DTR line transitions from the active to inactive state while the port is on online data mode, the port will drop to AT command mode. This is equivalent to issuing the AT Command: AT&D1.

Hangup
If the DTR line transitions from the active to inactive state while the port is on online data mode, the port will terminate the current call. This is equivalent to issuing the AT Command: AT&D2.

Initialisation string
Enter an initialisation string if required.

Click the Update button to save and commit changes. The main Circuit Switch Mode page will again be displayed.

6.5.2 Configuring for direct to single port mode

To select direct mode, in the upper table, set the **Operating mode** to **Direct to single port** and click the Update button to save and commit changes.

On models with more than one serial port, it may be desired to change the port that is selected for direct mode. To do this, click the  icon in the upper table. The port selection page, as shown in Fig. 6.32 will be displayed. Select the desired port from the drop-down box and click Update to set the change.

Fig. 6.32: Setting the direct mode port

6.5.3 Configuring for multiplexed mode

Multiplexed mode allows a remote user to dial in to the modem and select the port they wish to communicate with. Whereas **Direct to single port mode** fixes the port to be selected, multiplexed mode allows the selection to be made dynamically. This is suited to applications where multiple devices are attached to the modem's serial ports.

Furthermore, the PPP server (refer to section *Configuring for PPP server mode*) is also available as one of the multiplexer selections. This allows applications that normally only use serial data to dial in to the modem and create an IP connection to access modem's web server should any configuration changes need to be made.

Once a call is established in multiplexed mode, the modem will issue the following prompt:

```
CT Mux >
```

This indicates the modem is waiting for a port selection. To select a port, issue the command:

```
PORT=n<CR>
```

where n is the port number and <CR> is a carriage return. The PPP server is selected using the command:

```
PORT=PPP<CR>
```

> **Tip**
>
> For applications where the prompt text may interfere with serial protocols, it can be disabled using the **Menu visibility** option.

The multiplexer can support multiple port selections in a single call. Once a port has been selected, it can be deselected by issuing a special command sequence called the disconnect sequence. When received, this will cause the multiplexer to drop back to the menu prompt.

An example disconnect sequence is

```
<2 seconds delay>???<2 seconds delay>
```

> **Tip**
>
> The delay and character used in the disconnect sequence are configurable.

To select multiplexed mode, in the upper table of the Circuit Switched Data page, set the **Operating mode** to **Multiplexed** and click Update to set the change. The display will update to be similar to that shown in Fig. 6.33, the summary data will provide a summary of the multiplexed mode settings.

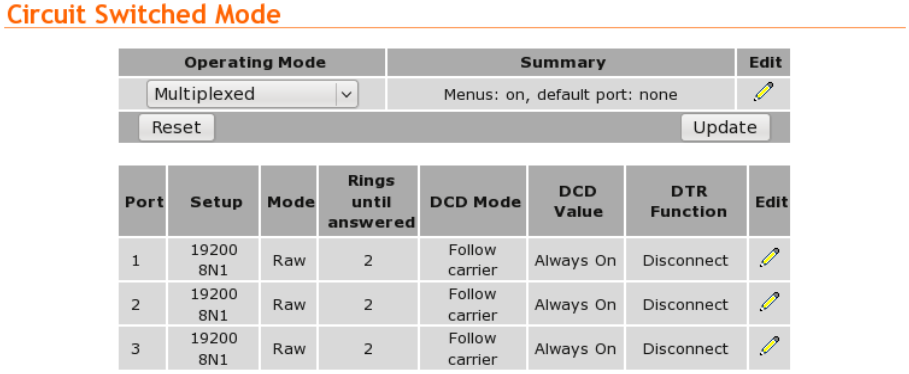


Fig. 6.33: Setting the direct mode port

To configure multiplexed mode, click the  icon in the upper table. The multiplexed mode configuration page, as shown in Fig. 6.34 will be displayed.

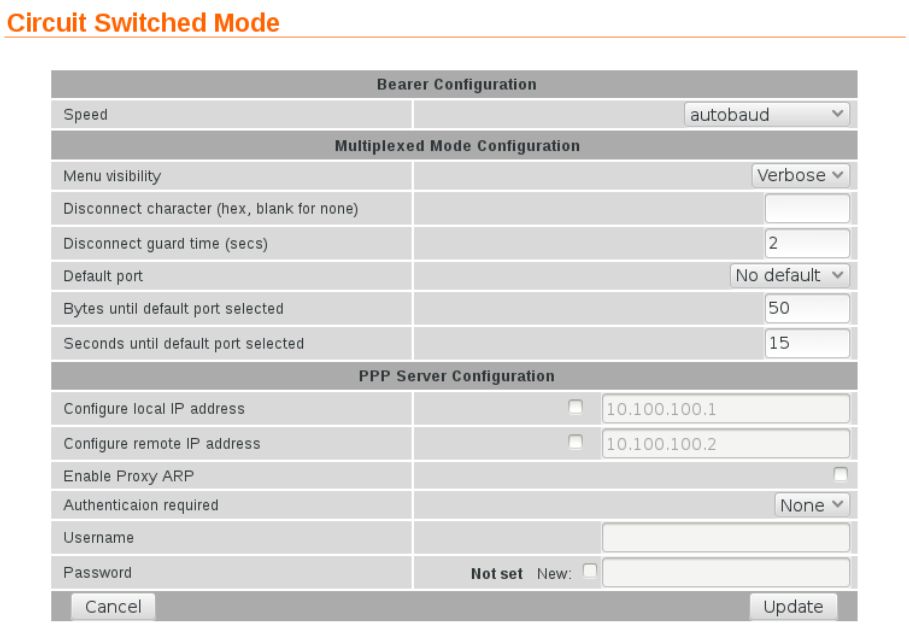


Fig. 6.34: Configuring multiplexed mode

The following options can be configured for multiplexed mode:

Bearer Configuration Speed
Choose the operating baud rate for the connection to the wireless network. The default and recommended setting is autobaud. This will automatically set the baud rate.

> **Tip**
>
> Changing the baud rate value for the wireless connection usually has not affect. Connection problems may occur if the baud rates do not match. It is for this reason the recommended setting is autobaud.

Multiplexed Mode Configuration

Menu visibility
Depending on the application, it may not be desirable to have the multiplexer present menu prompts to the remote modem. This field controls the display of menus:

Verbose
The modem will send prompts and status updates to the remote user.

Silent
No prompts will be displayed.

Disconnect character
This field determines the character used in the disconnect sequence discussed above. The default is a question mark (?), which is entered as 3f hex. To disable the disconnect feature, clear all text in this field.

Disconnect guard time
This field determines the idle time around the disconnect sequence discussed above. The value entered is in seconds.

Default port
In some applications, it may be desirable to have one of the multiplexer's ports selected automatically if no valid PORT= command has been received within a specified amount of time or specified number of bytes. This dropdown box selects the default port.

Bytes until default port selected
Where **Default port** is not set to **No default**, this field determines the number of bytes before the default port is selected.

Seconds until default port selected:
Where **Default port** is not set to **No default**, this field determines the seconds that can elapse before the default port is selected.

PPP Server Configuration Local IP address
Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Remote IP address
Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP
Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication required
This fields sets the required level of authentication for remote users connecting to the modem. Available options are:

None
No authentication will be required.

PAP
Authentication will be required using the PAP protocol.

CHAP
Authentication will be required using the CHAP protocol.

Username
Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password
Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** checkbox and enter the password in the adjacent field.

Click Update to save any changes.

6.5.4 Configuring for PPP server mode

To select PPP server mode, in the upper table of the Circuit Switched Data page, set the **Operating mode** to **PPP server** and click Update to set the change. The display will change to that shown in Fig. 6.35, notice the port list is no longer displayed. As the connection to the modem is now over a packet based PPP connection the ports must be accessed via the Serial Server. For details on the Serial Server refer to the *Serial Server* Chapter.

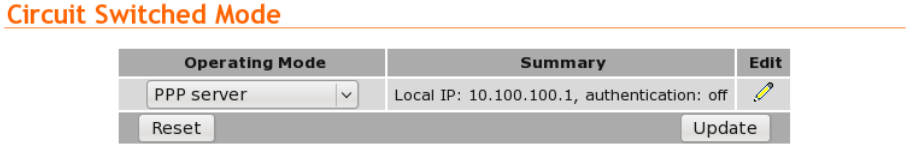


Fig. 6.35: PPP server configuration

To configure PPP server mode, click the icon in the upper table. The PPP server configuration page, as shown in Fig. 6.36 will be displayed.

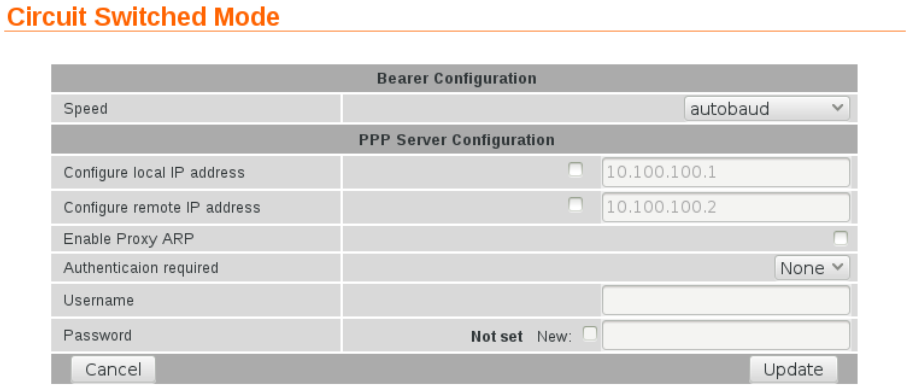


Fig. 6.36: PPP server configuration

The following options can be set for PPP mode:

Bearer Configuration Speed
Choose the operating baud rate for the connection to the wireless network. The default and recommended setting is autobaud. This will automatically set the baud rate.

> **Tip**
>
> Changing the baud rate value for the wireless connection usually has no effect. Connection problems may occur if the baud rates do not match. It is for this reason the recommended setting is autobaud.

PPP Server Configuration Local IP address
Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Remote IP address
Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP
Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication required
This fields sets the required level of authentication for remote users connecting to the modem. Available options are:

None
No authentication will be required.

PAP
Authentication will be required using the PAP protocol.

CHAP
Authentication will be required using the CHAP protocol.

Username
Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password
Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** checkbox and enter the password in the adjacent field.

Click the Update button to save and commit changes.

6.5.5 PPP Dial-out

To select PPP dialout mode, in the upper table of the Circuit Switched Data page, set the **Operating mode** to **PPP dialout** and click Update to set the change. The display will change to that shown in Fig. 6.35, notice that as with to PPP server the port list is no longer displayed. As the connection to the modem is now over a packet based PPP connection the ports must be accessed via the Serial Server. For details on the Serial Server refer to the *Serial Server* Chapter.

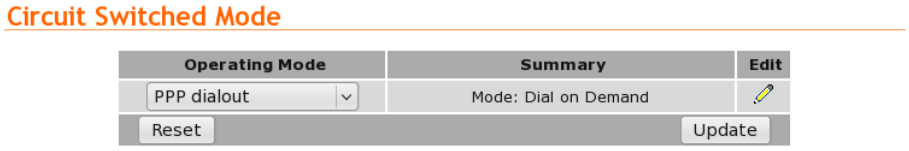


Fig. 6.37: PPP dialout configuration.

To configure PPP server mode, click the icon in the upper table. The PPP dialout configuration page, as shown in Fig. 6.38 will be displayed.

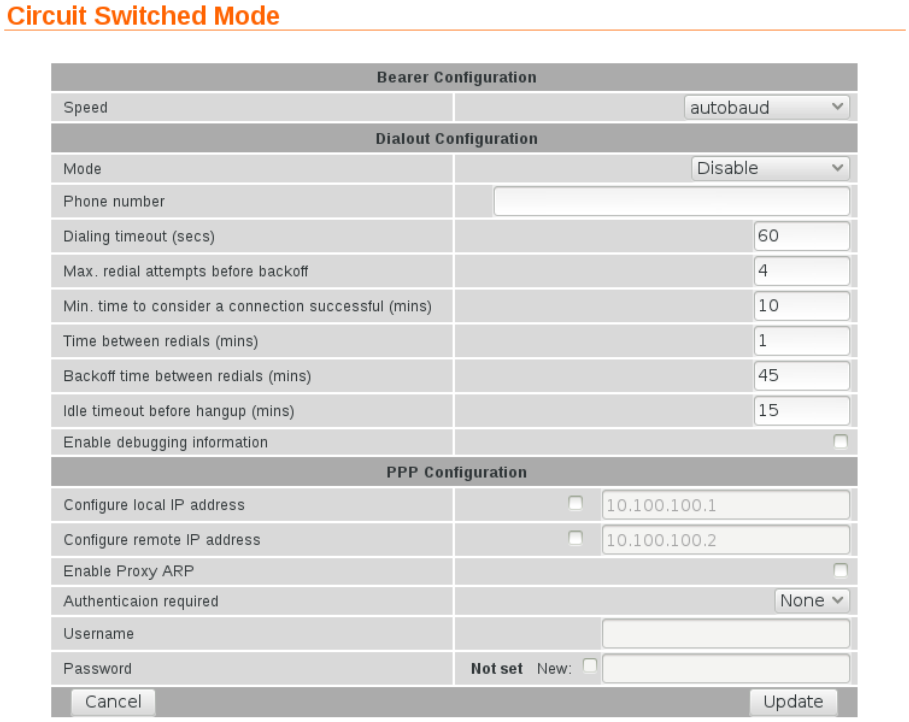


Fig. 6.38: PPP dialout configuration.

The following options can be set for PPP Server dialout configuration:

Bearer Configuration Speed
: Choose the operating baud rate for the connection to the wireless network. The default and recommended setting is autobaud. This will automatically set the baud rate.

> **Tip**
>
> Changing the baud rate value for the wireless connection usually has no effect. Connection problems may occur if the baud rates do not match. It is for this reason the recommended setting is autobaud.

Dialout Configuration Mode
This field sets the operating mode. Available options are:

Disable
Disable dial out.

Manual
The connection is controlled manually by clicking the Connect and Disconnect buttons which are added to the Circuit Switch Data page when this mode is selected.

On demand
The connection is made when data is sent to the interface.

Always connect
The connection is permanently established.

> **Warning**
>
> Care should be taken when selecting the operating mode as incorrect setting could result in excessive data charges.

Phone number
The number to call.

Dialing timeout
The time in seconds to wait for a connection after dialling.

Max. redial attempts before backoff
Set the number of failed dialling attempts after which the time between dialling will be increased. This back-off prevents continuously dialling at a fast rate possibly incurring large call costs.

Min. time to consider a connection successful
The minimum connection time in minutes which is considered a successful connection.

Time between redials
The time in minutes to wait after a failed dial attempt before redialling.

Backoff time between redials
The time in minutes to wait to redial after the back-off count has been reached.

Idle timeout before hangup
The connection is considered idle when no data has been transmitted or received for this time in minutes. Once the idle time is reached the connection will be terminated.

Enable debugging information
If enabled debugging information is written to the log. This can assist in diagnosing connection problems.

PPP Server Configuration Local IP address
Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Remote IP address
Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the **Local IP address**.

Enable Proxy ARP
Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication required
This fields sets the required level of authentication for remote users connecting to the modem. Available options are:

None
No authentication will be required.

PAP
Authentication will be required using the PAP protocol.

CHAP
Authentication will be required using the CHAP protocol.

Username
Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password
Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

Click the Update button to save and commit changes.

6.6 SMS

SMS triggers provide a mechanism to report and change the state of the unit. For example change the Wireless operating mode, reboot the modem and request a status summary. Each SMS trigger can individually be enabled and disabled and the text trigger can be defined for each trigger. Access control is provided to control which numbers have access to the SMS triggers.

To access the SMS Triggers select *Wireless* → *SMS* a page similar to that shown in Fig. 6.39 and Fig. 6.40 will be displayed, the second figure is for a model with GPIO and includes GPIO SMS triggers.

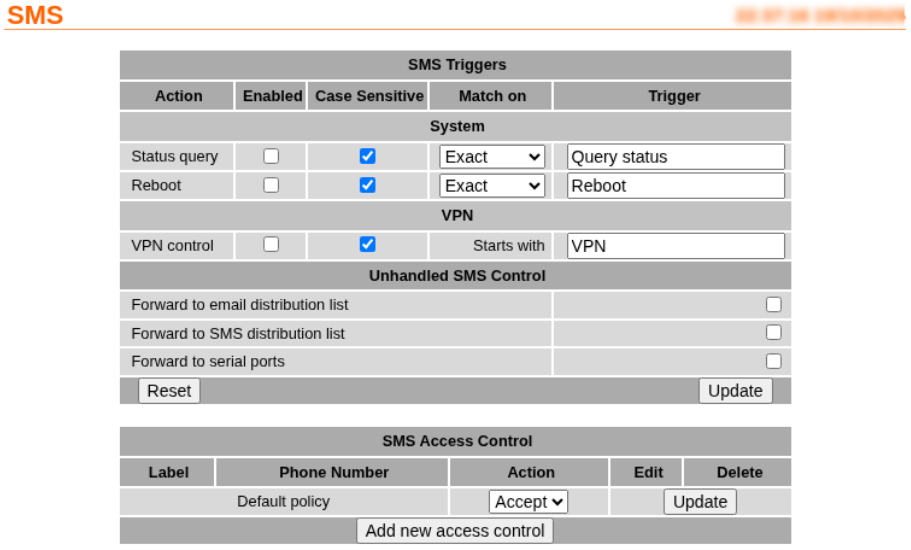


Fig. 6.39: SMS Triggers configuration page.

6.6.1 Trigger configuration

The fields below, found in the **SMS Triggers** table, configure an individual trigger:

SMS Triggers

Action
The SMS actions are separated into several sections, the number of sections varies with each model. The actions are described below:

System

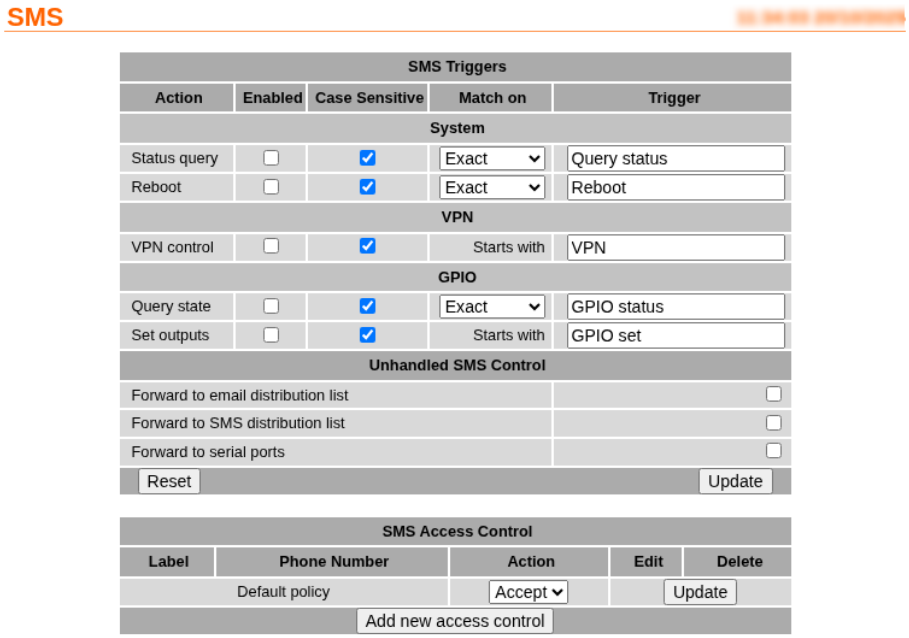


Fig. 6.40: SMS Triggers configuration page for a model with GPIO.

Status query
Query the current state. An SMS will be returned providing current status information.

Reboot
Initiate a reboot.

Wireless Packet mode
Switch to packet mode.

CSD mode
Switch to Circuit Switched Data (CSD) mode.

VPN

VPN control
Start, stop and re-start VPNs. The VPN command has 2 parameters, action and tunnel and is of the form "VPN <action> <tunnel>". The parameters are:

action
One of the following:

start
Start the specified tunnel.

stop
Stop the specified tunnel.

restart
Stop and then start the specified tunnel.

tunnel
One of the following:

All
Apply the action to all configured tunnels.

SSL
Apply the action to only the SSL VPN.

<label>
Apply the action only to the tunnel with the specified label.

GPIO
General Purpose Input and Outputs (GPIO).

Query state
Report the current state of the Inputs and Outputs.

Set outputs
Set the state of the outputs. The output is referenced by its index number, only referenced outputs will change.

The form of the command is:

"GPIO set <index>=<o/c>"

where:
o: Sets the output <index> to Open.

c: Sets the output <index> to Closed.

Enabled
Set this checkbox to enable the trigger.

Case sensitive
Set this checkbox to make the trigger case sensitive. If not set, the trigger will match regardless of the case of the characters in the SMS.

Match on
This value determines how an incoming SMS will be searched to find a match for this trigger. The following match modes can be used:

Exact
The trigger will match if the content of the SMS is identical to the **Trigger** field.

Contains
The trigger will match if the content of the SMS contains the **Trigger** field.

Starts with
The trigger will match if the content of the SMS starts with the **Trigger** field.

Trigger
This is the text that will be used, in conjunction with the **Match on** field, to determine whether an SMS is for this trigger.

Unhandled SMS Control
Set the action for SMS which do not match any of the enabled triggers. Options:

Forward to email distribution list
Forward the SMS as an email to all the addresses contained in the email distribution list.

Forward to SMS distribution list
Forward the message to all of the numbers listed in the SMS distribution list

Forward to serial ports
Message will be sent to any serial ports configured in modem emulation mode.

Click the Update button to save and commit changes.

6.6.2 SMS Access control

When the modem receives an SMS, it also receives the phone number which sent the message. The SMS Access control allows source phone numbers to be verified to ensure the sender is authorised to access the modem.

Each access control is specified by setting a phone number and an associated action. The action for each control can be:

Drop
Messages from the phone number will be dropped and not processed by the modem.

Allow
: Messages from the phone number will be accepted and processed by the modem.

The default policy determines the action to be taken when no specific access control matches a phone number. The default policy is **Allow**, however, this can be set to **Drop** for stricter level of control.

Setting the default policy to allow

This example describes setting the default policy to **Allow** then adding an entry to blacklist a particular number.

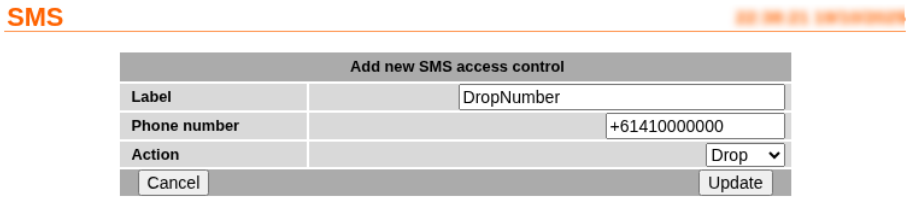


Fig. 6.41: SMS Triggers reject entry

1. In the section titled **SMS Access Control** set the **Action** for the **Default policy** to **Accept**.
2. Click **Update** to set the changes.
3. Click the **Add new SMS access control** button.
4. In the entry form, (Fig. 6.41) enter:
    1. A label for the new entry.
    2. Enter the phone number (this should be entered with the full country prefix eg. +61410000000).
    3. Set the **Action** to **Drop**.
5. Click the **Update** button to set the changes.
6. Repeat the steps above to add further numbers.

When complete the page will include the number to be dropped, as shown in Fig. 6.42.

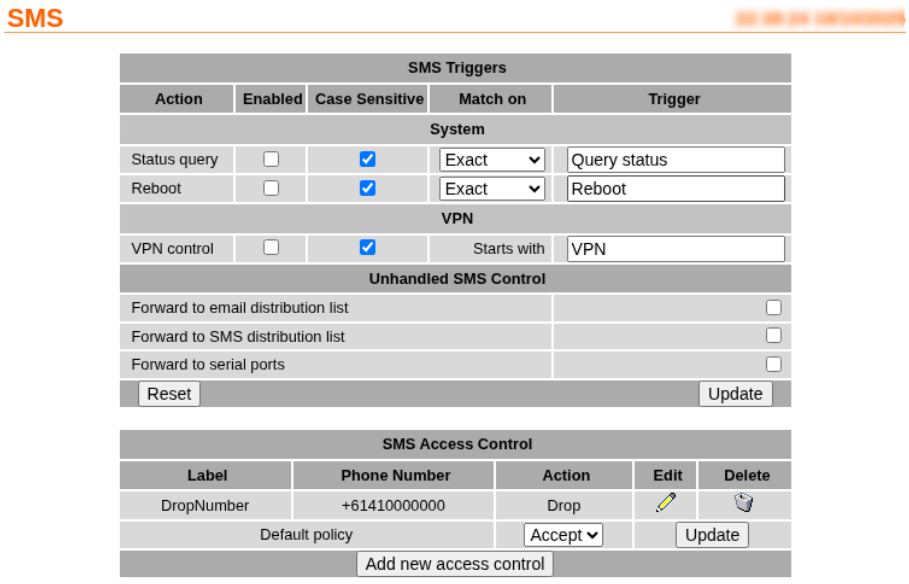


Fig. 6.42: SMS Triggers number to drop added

Deleting an Entry

To delete an entry click the icon a dialogue box similar to that shown in Fig. 6.43 will be displayed. Click the OK button to remove the entry.

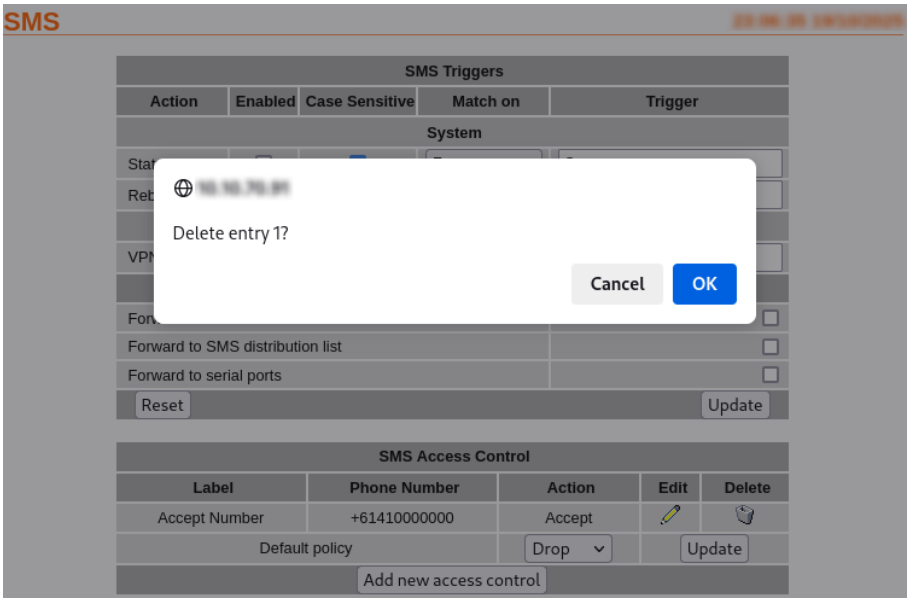


Fig. 6.43: Deleting the Drop entry.

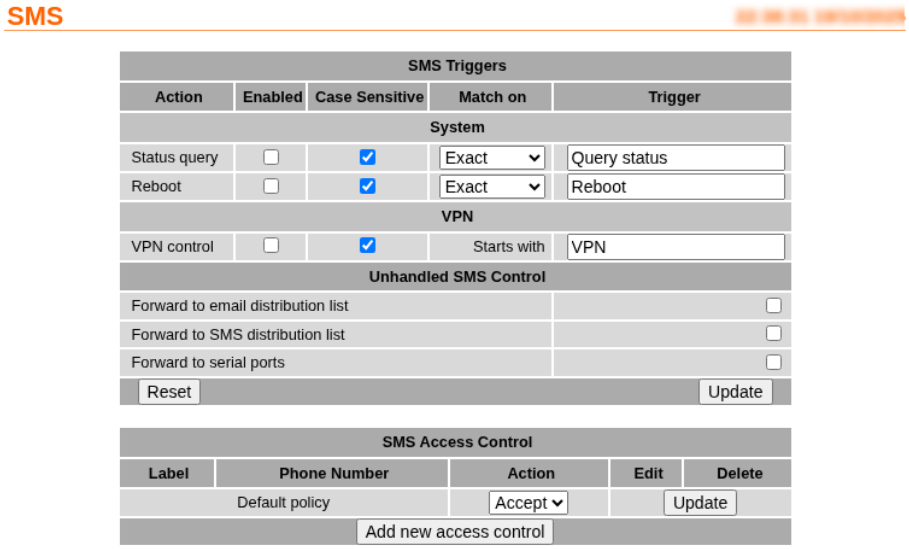


Fig. 6.44: The Drop entry has been deleted.

Setting the default policy to drop

This example describes setting the default policy to **Drop** then adding an entry to allow a specific number.

1. In the section titled **SMS Access Control** set the **Action** for the **Default policy** to **Drop**.
2. Click **Update** to set the changes. The page will look similar to that shown in Fig. 6.45
3. Click the **Add new SMS access control** button.
4. In the entry form (Fig. 6.46) enter:
    1. A label for the new entry.

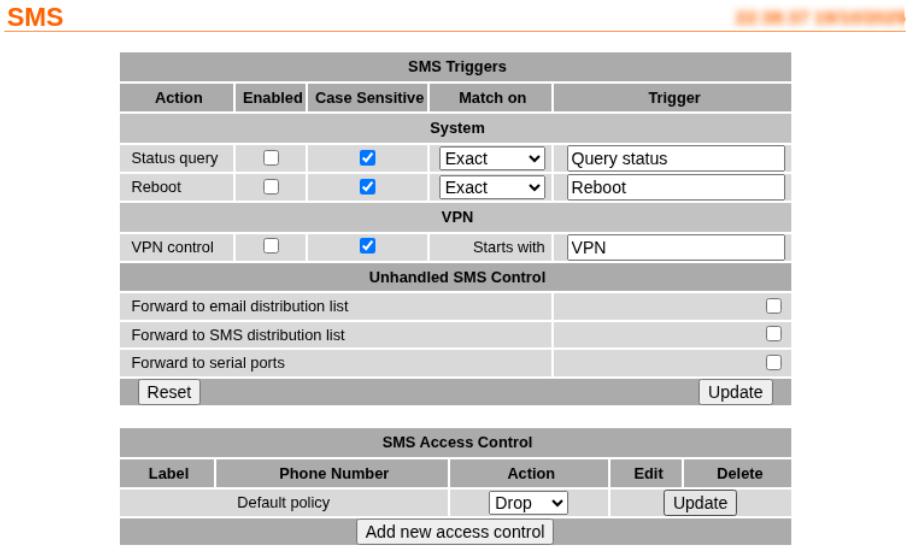


Fig. 6.45: SMS access control default policy set to Drop.

2. Enter the phone number (this should be entered with the full country prefix eg. +61410000000).
3. Set the **Action** to **Allow**.

5. Click the **Update** button to set the changes.
6. Repeat the steps above to add further numbers.

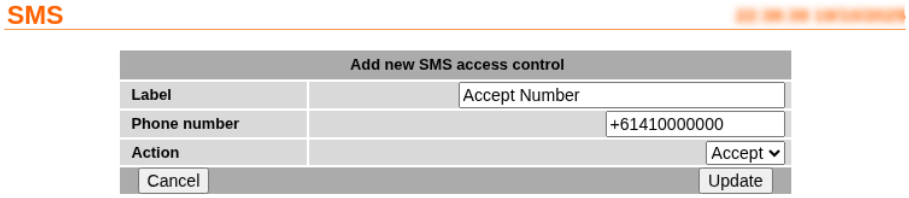


Fig. 6.46: SMS Triggers accept entry

When complete the page will include the number to be accepted, as shown in Fig. 6.47.

Editing an Entry

To edit an entry click the  icon and complete the edits. Click the Update button to save and commit changes.

6.6.3 SMS Examples

The examples listed below will all use the same configuration of the SMS triggers which is shown in Fig. 6.48 on the following page. A Model with GPIO has been used so that examples of the GPIO can be demonstrated. All SMS are sent from a standard mobile to the phone number of the SIM installed in the unit.

Status Query

The status query SMS is issued as follows:

SMS

Query status

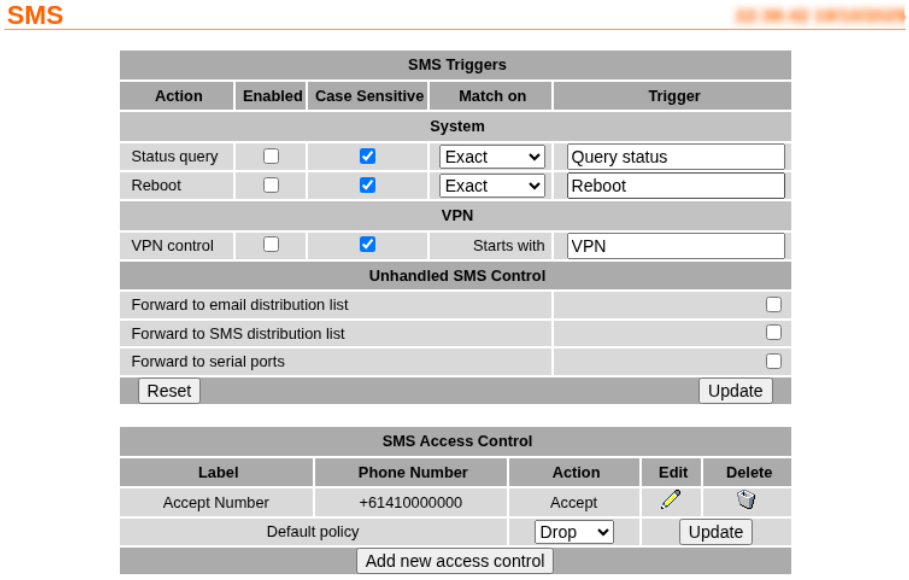


Fig. 6.47: SMS Triggers number to accept added

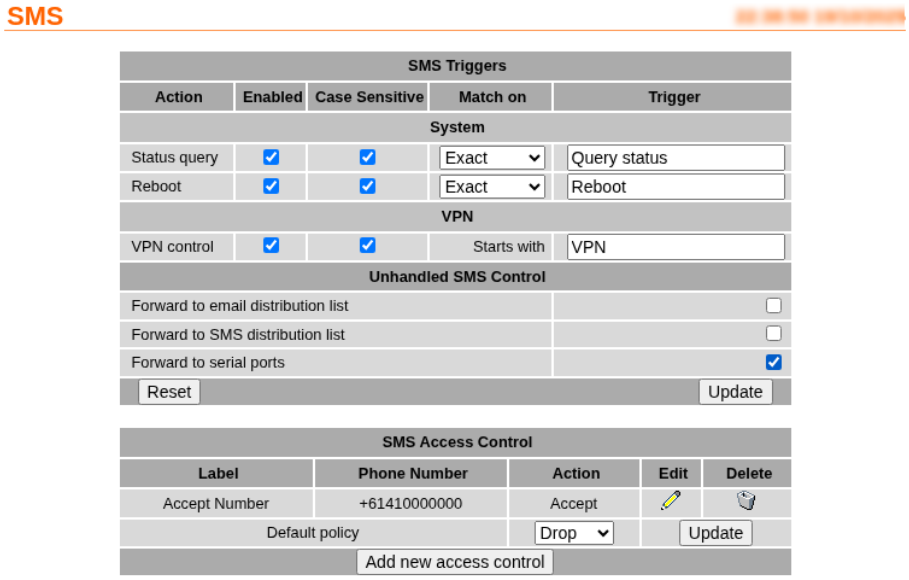


Fig. 6.48: SMS Example configuration.

The modem responds with:

SMS

Host:S2000-ff-ff-00, Uptime:14003399, Temp:37.25, RSSI:20, Mode:Pkt, State:Connected (10.192.168.23), LAN:Up (10.10.10.10)

The meaning of the fields within the message are:

Host
The host name of the responding unit.

Uptime
The up time in seconds.

Temp
The current temperature in Celsius.

RSSI
The current Receive Signal Strength Indicator (RSSI) reading.

Mode
The current operating mode, either packet (Pkt) or Circuit Switched Data (CSD)

State
The state of the connection. If the connection mode is packet the wireless IP address is also displayed.

LAN
The state and if active the IP address of the LAN.

Reboot

In this example the unit will be rebooted.

The reboot SMS is issued as follows:

SMS

Reboot

A shut-down sequence will be initiated and the unit will reboot. This will take approximately 5 minutes during which time the unit will be disconnected from the wireless network and not accessible.

Wireless Mode

In this example the unit will be switched from packet mode to circuit switched data mode and back to packet mode. From the Status query example above the unit is currently in packet mode so the first SMS will be to switch to CSD mode.

The Wireless mode SMS is issued as follows:

SMS

Mode CSD

Now to check the mode a Query status message is sent:

SMS

Query status

The modem responds with a message similar to the following:

SMS

Host:S2000-ff-ff-00, Uptime:14005447, Temp:37.25, RSSI:20, Mode:CSD, State:Offline, LAN:Up (10.10.10.10)

To switch back to packet mode another Wireless SMS is sent:

SMS

Mode packet

Again to check the mode a Query status message is sent:

SMS

Query status

The modem responds with a message similar to the following:

SMS

Host:S2000-ff-ff-00, Uptime:14005664, Temp:37.25, RSSI:20, Mode:Pkt, State:Connected (10.192.168.32), LAN:Up (10.10.10.10)

VPN Control

The VPN control SMS is issued as follows:

SMS

VPN restart ALL

This SMS command will restart all enabled VPNs.

To restart only the VPN labelled test the following SMS command would be issued:

SMS

VPN restart test

GPIO

Two GPIO SMS commands are available the first reports the status of all inputs and outputs while the second provides output control.

To report the GPIO status the following SMS command is issued:

SMS

GPIO status

The response will be similar to:

SMS

S2000-ff-ff-00:Input-1=disabled, Input-2=disabled, Output-1=disabled, Output-2=disabled

In this case all of the inputs and outputs are reported as disabled. If the inputs and outputs are now enabled and the SMS GPIO status command is re-sent the following response is received:

SMS

S2000-ff-ff-00:Input-1=open, Input-2=open, Output-1=open, Output-2=open

To change the state of the outputs to closed the following command is sent:

SMS

GPIO set 1=c 2=c

A status message can now be sent to check on the result:

SMS

GPIO status

The response will be similar to:

SMS

S2000-ff-ff-00:Input-1=open, Input-2=open, Output-1=closed, Output-2=closed

The state of the two outputs has changed from “open” to “closed”.

CHAPTER

SEVEN

DSL

The section explains the procedure for configuring the DSL interface in order to establish an ADSL or VDSL connection. To access the configuration page for the DSL interface, click on the *DSL* tab of the main menu. The DSL Network configuration page will be displayed as shown in Fig. 7.1.

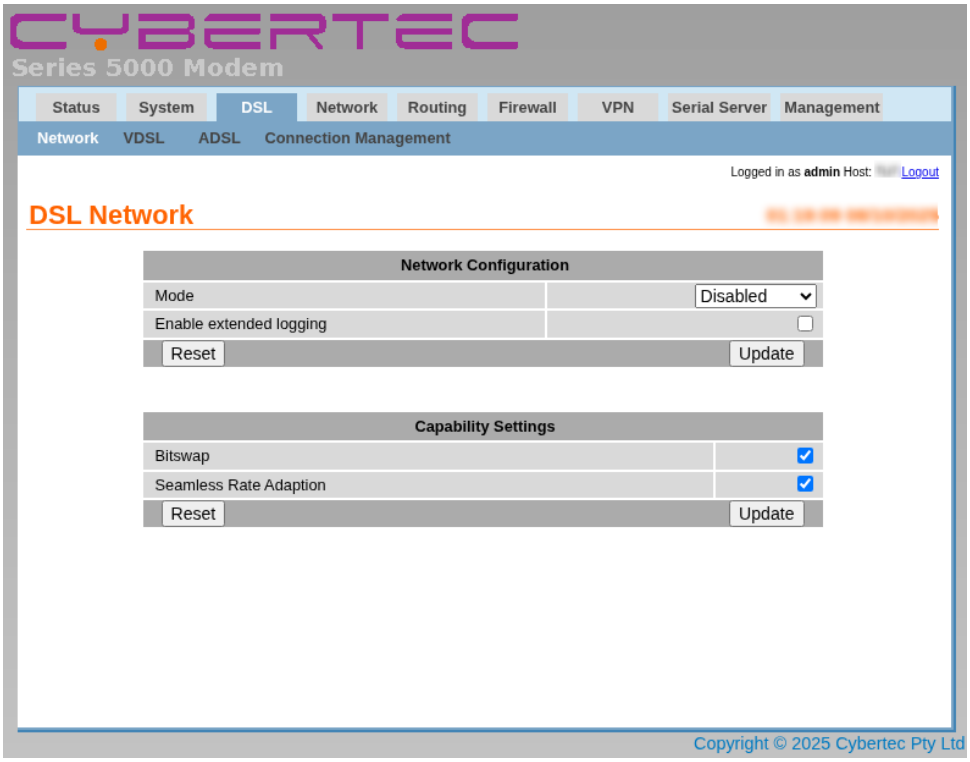


Fig. 7.1: DSL main configuration page.

7.1 Configure the DSL Network

The DSL Network options are used to set the operating mode, and capability settings. To display the DSL Network page select *DSL* → *Network* from the menu. When selected the page similar to that shown in Fig. 7.2 will be displayed.

7.1.1 Network Configuration

The configuration options are:

Mode
Set the operating mode of the DSL interface. The following modes of operation are supported, select from:

Disabled
The DSL interface is shut-down. No data connections are possible over the DSL interface.

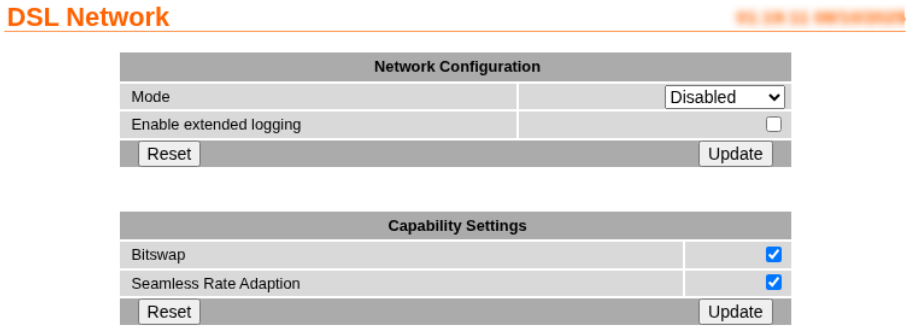


Fig. 7.2: DSL-Network.

VDSL/ADSL
Enable both VDSL and ADSL capabilities. The unit will auto-detect and use the appropriate DSL technology based on the line conditions.

VDSL Only
Enable only VDSL capabilities. The unit will only attempt VDSL connections.

ADSL Only
Enable only ADSL capabilities. The unit will only attempt ADSL connections.

Enable extended logging
Check to enable extended logging for the DSL interface. This option is useful if connection problems are encountered.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.1.2 Capability Settings

The configuration options are:

Bitswap
Bit swap process enables the connection to either change the number of bits assigned to each individual sub-channel or if necessary increase the power level whilst still maintaining the data flow. If bit-swapping were not enabled, and a noise burst were to prevent a sub-channel being able to transmit its allocated number of bits the connection would lose sync and would need to re-train.

Seamless Rate Adaption
Is a feature whereby the data transmission rate is adjusted in real-time in order to adapt to changing line and network conditions in order to avoid dropping the connection. Data transmission is maintained while during the rate changes.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.2 VDSL Configuration

To access the VDSL configuration, select *DSL* → *VDSL* from the menu. The screen shown in Fig. 7.3 will be displayed.

7.2.1 Connection Configuration

The first section of the page is for the Connection Configuration. In order for the modem to be able to establish an VDSL connection, the details of the connection must be set up in a connection profile. This section details the process of adding, editing and deleting a VDSL connection profile. While most configurations will only need one configuration profile, multiple profiles are supported. Once the profile or profiles have been configured one can be selected as the active profile.

By default packet mode is disabled and no profiles are configured.

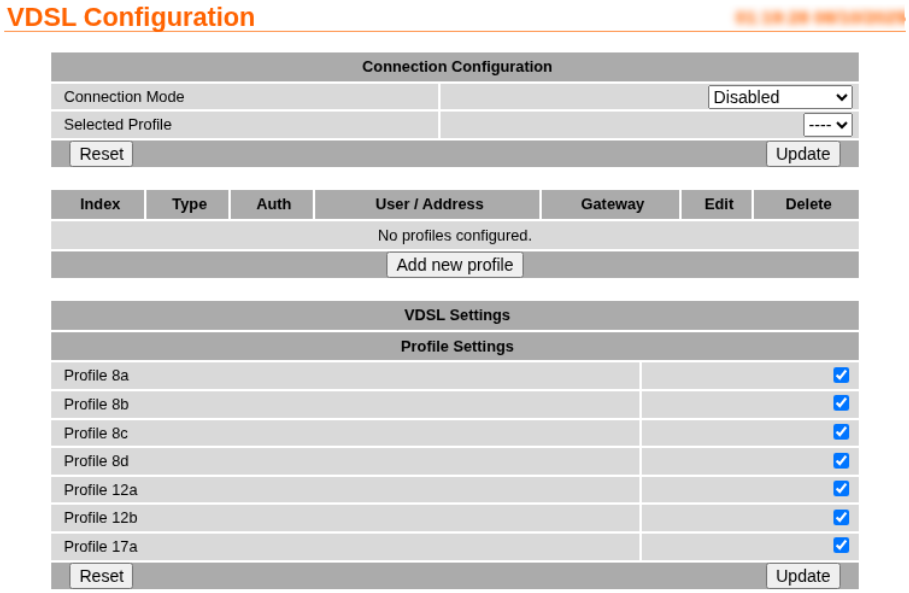


Fig. 7.3: Main VDSL Configuration page.

Connection Mode
The packet connection mode options:

Disabled (Default)
Packet connections are disabled.

Always Connect
Establish and maintain a packet connection.

Automatic
Establish a connection only when VRRP master. In order for this to function VRRP must also be configured, for details refer to *Virtual Router Redundancy Protocol (VRRP)* section in the *Routing* chapter.

Profile
Select the index of a defined profile. Refer to next section on how to add connection profiles.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.2.2 Profile Management

To add an VDSL profile click the Add new profile button, the Add New Profile page as shown in Fig. 7.4 will be displayed.

The profile contains the details for connecting to a particular VDSL service.

> **Note**
>
> The network provider will specify the required settings for completing a connection profile. The provider may not supply a user-name and password if network authentication is not required. In this case set the **Authentication** to **None**.

The first section relates to VLAN settings for the DSL connection, and is common to all connection types. The options are:

VDSL Configuration Settings

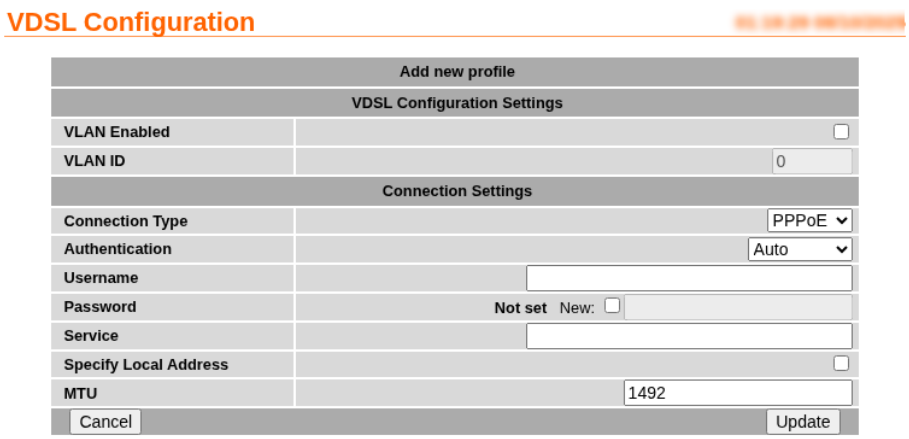


Fig. 7.4: Add new VDSL profile.

VLAN Enabled
Check to enable VLAN over the DSL interface.

VLAN ID
Enter the VLAN ID for use over the DSL interface.

The options within the second section listed under the title Connection Settings will changed depending on the selected connection type. The first step is to select the connection type from the drop-down list, the options are:

Connection Type
The VDSL connection type is selected from the drop-down list. Once selected the options will be changed to those relevant for the selected connection type.

PPPoE
Point to Point Protocol over Ethernet is a method of encapsulating PPP frames within Ethernet frames.

IPoE
Internet Protocol over Ethernet is a method of encapsulating IP datagrams with Ethernet frames without using PPPoE.

Bridged
Creates a direct connection between the LAN (Ethernet) interface and the DSL interface.

Once The connection type has been selected refer to the appropriate section below for the relevant settings.

Connection Type PPPoE

When Point to Point Protocol over Ethernet (PPPoE) is selected as the connection type the PPPoE options will be shown, refer to Fig. 7.5 for details.

Connection Type

PPPoE
The PPPoE option is selected.

Authentication
For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None
No authentication is performed.

PAP
The Password Authentication Protocol is used.

CHAP
The Challenge-Handshake Authentication Protocol is used.

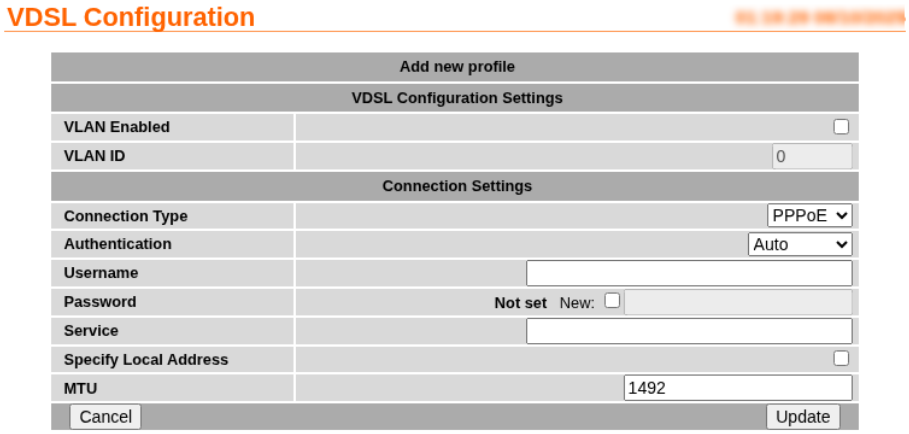


Fig. 7.5: Add new VDSL profile with connection type PPPoE.

Auto (Default)
The authentication protocol is automatically determined.

MS-Chap
The Microsoft version of the Challenge-Handshake Authentication Protocol (CHAP) is used.

Username
For connections where the Authentication is not set to None, this is the user-name the modem will use to authenticate.

Password
For connections where the Authentication is not set to None, this is the password the modem will use to authenticate. In order to set a password click the check box marked New then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

Service
The service string.

MTU
Setting for the Maximum Transmission Unit of the DSL interface.

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type IPoE

When Internet Protocol over Ethernet (IPoE) is selected as the connection type the IPoE options will be shown, refer to Fig. 7.6 for details.

Connection Type

IPoE
The IPoE option is selected.

Address Mode

Static
Set a static address IP address for the DSL interface

Address
The IP address for the interface.

Netmask
The netmask for the interface.

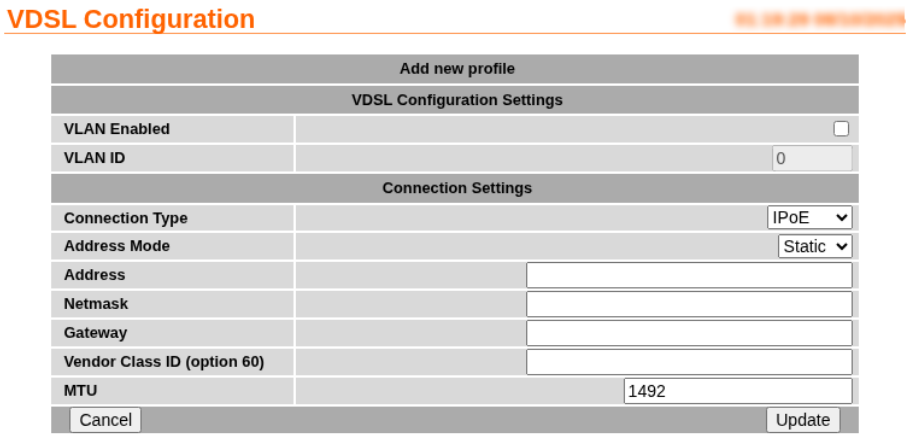


Fig. 7.6: Add new VDSL profile with connection type IPoE.

Gateway
The gateway address for the interface.

DHCP
The IP address settings for the interface will be set dynamically.

MTU
Setting for the Maximum Transmission Unit of the DSL interface.

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type Bridged

When Bridged is selected as the connection type there are no configurations settings required, refer to Fig. 7.7 for details.

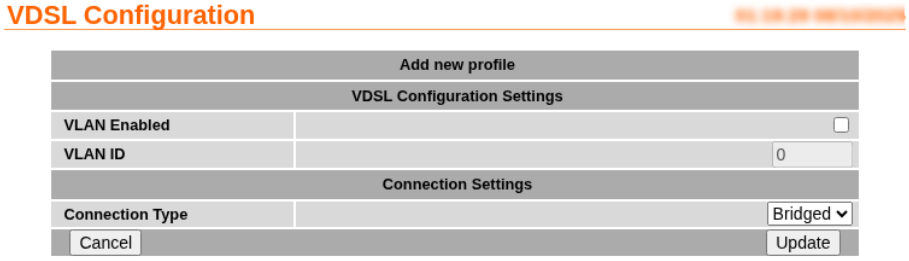


Fig. 7.7: Add new VDSL profile with connection type bridge.

Connection Type

Bridged
Bridged is selected

No settings required for bridged mode.

7.2.3 Example of Adding a VDSL Profile

In this example a profile will be added with the following details:

VDSL Connection Settings:

VLAN
Enabled

VLAN ID
100

Connection Settings:

Connection Type
IPoE :Address Mode: Static :Address: 10.10.80.2 :Netmask: 255.255.255.0 :Gateway: 10.10.80.1

MTU
1492

To access the VDSL configuration, select *DSL → VDSL Mode* from the menu, a page as shown in Fig. 7.3 will be displayed. Assuming no profiles have been configured the profiles section of the page will be as shown in Fig. 7.8.

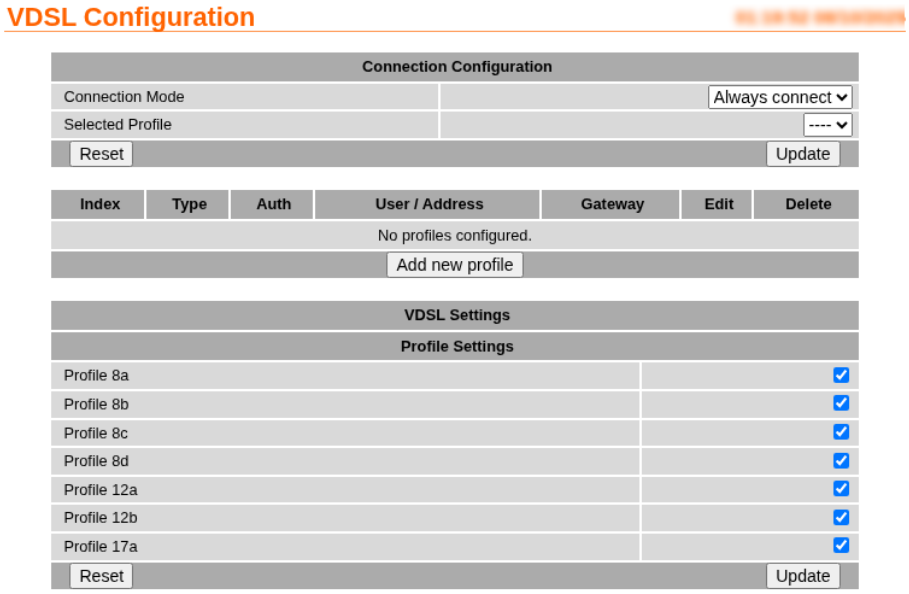


Fig. 7.8: VDSL with no profiles.

To add an VDSL profile click the Add new profile button, the Add New Profile page as shown and the details as listed above can be entered as shown in Fig. 7.9.

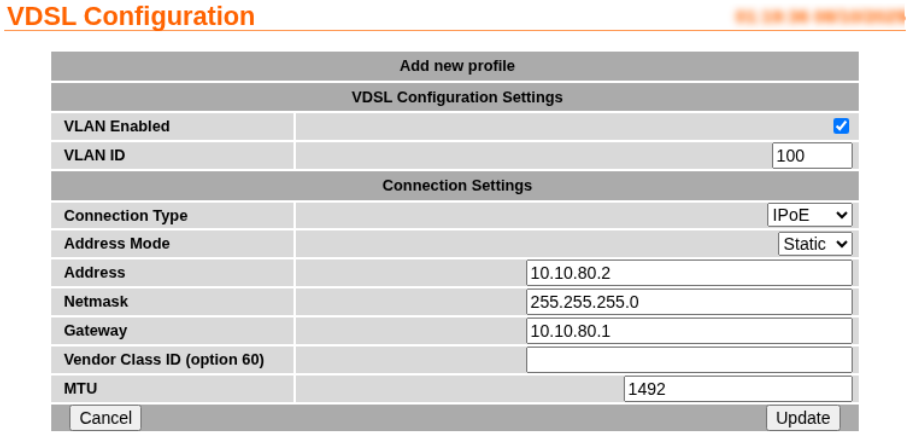


Fig. 7.9: Example of adding a VDSL profile configuration.

Once the profile has been entered click the Update button to save and commit changes.

The VDSL page will be shown again, and the new profile will be included in the profiles list, as shown in Fig. 7.10.

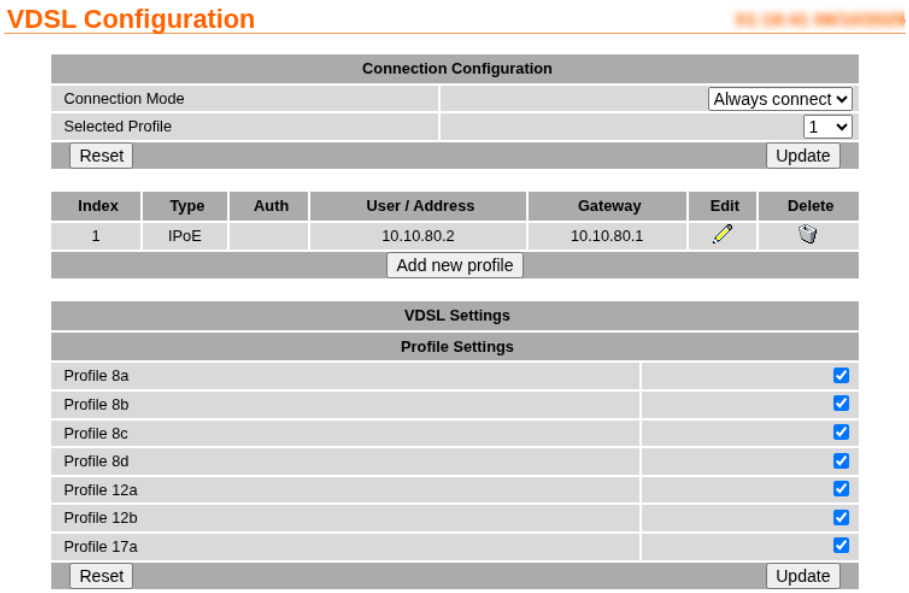


Fig. 7.10: Main VDSL page with newly added profile.

Within the Connection Configuration section the profile should be selected as the active profile. To enable the connection change the Connection Mode from Disabled to Always connect.

7.2.4 Example of Editing a VDSL Profile

To edit an existing profile click on the  icon located in the Edit column for the profile to be edited. A page similar to add profile page, which includes the details for the profile will be displayed.

The edit profile page for the profile entered in the example above are shown in Fig. 7.11.

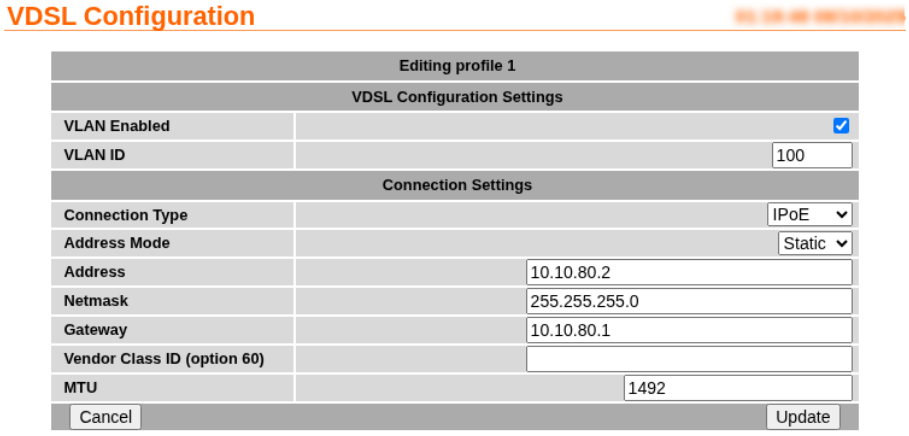


Fig. 7.11: Edit VDSL profile example.

Once the profile has been entered click the Update button to save and commit changes. To abort the changes and leave the profile unchanged click the Cancel button.

7.2.5 Example of Deleting a VDSL Profile

A profile can be deleted by clicking the icon located in the Delete column for the profile to be deleted. A dialogue box will shown requesting confirmation of the deletion, Click the OK button to proceed with the deletion or click the Cancel button to abort the deletion. Fig. 7.12 illustrations the deleting a profile entered in the example above.

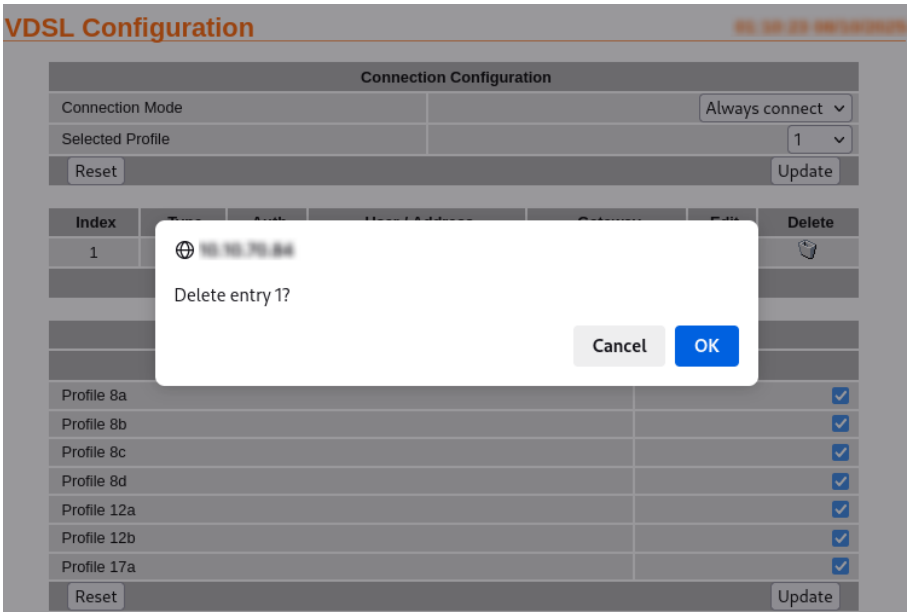


Fig. 7.12: Deleting a VDSL profile.

After confirming the deletion of the profile the main VDSL will be shown and will be similar Fig. 7.13.

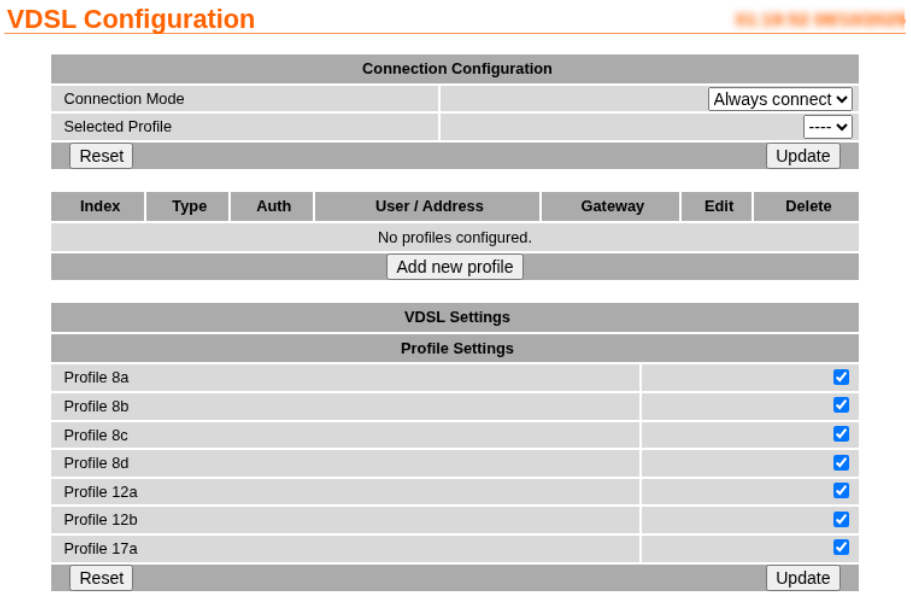


Fig. 7.13: Profile list after deleting the VDSL profile.

7.3 ADSL Configuration

To access the ADSL configuration, select *DSL* → *ADSL* from the menu. The screen shown in Fig. 7.14 will be displayed.

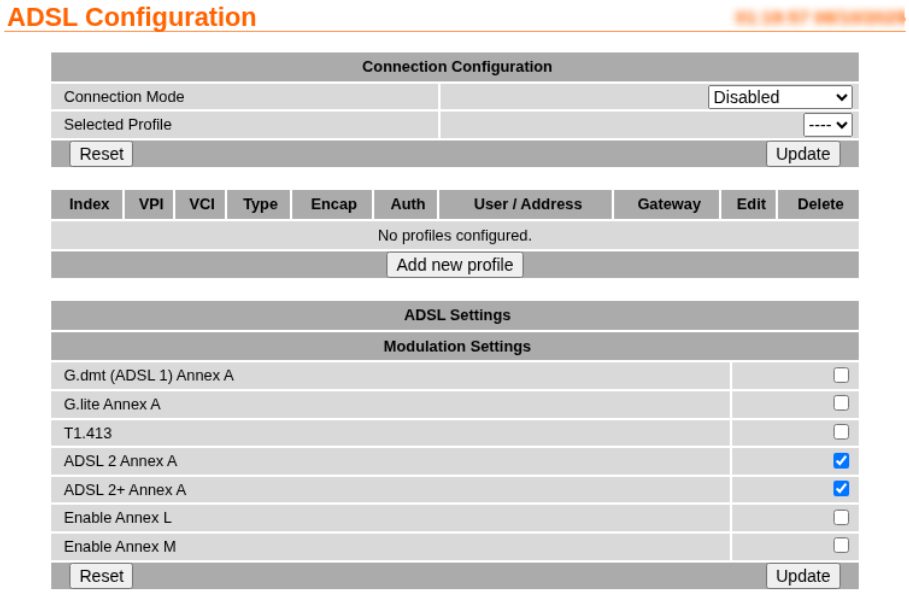


Fig. 7.14: Main ADSL Configuration page.

7.3.1 Connection Configuration

The first section of the page is for the Connection Configuration. In order for the modem to be able to establish an ADSL connection, the details of the connection must be set up in a connection profile. This section details the process of adding, editing and deleting a ADSL connection profile. While most configurations will only need one configuration profile, multiple profiles are supported. Once the profile or profiles have been configured one can be selected as the active profile.

By default packet mode is disabled and no profiles are configured. The options are:

Connection Mode:

Disabled
: Packet connections are disabled.

Always Connect
: Establish and maintain a packet connection.

Automatic
: Establish a connection only when VRRP master. In order for this to function VRRP must also be configured, for details refer to *Virtual Router Redundancy Protocol (VRRP)*

Profile
: Select the index of a defined profile. Refer to next section on how to add connection profiles.

Click the Update button to save and commit changes. Click the Reset button to revert to the original settings.

7.3.2 Profile Management

To add an ADSL profile click the Add new profile button, the Add New Profile page as shown in Fig. 7.15 will be displayed.

The profile contains the details for connecting to a particular ADSL service.

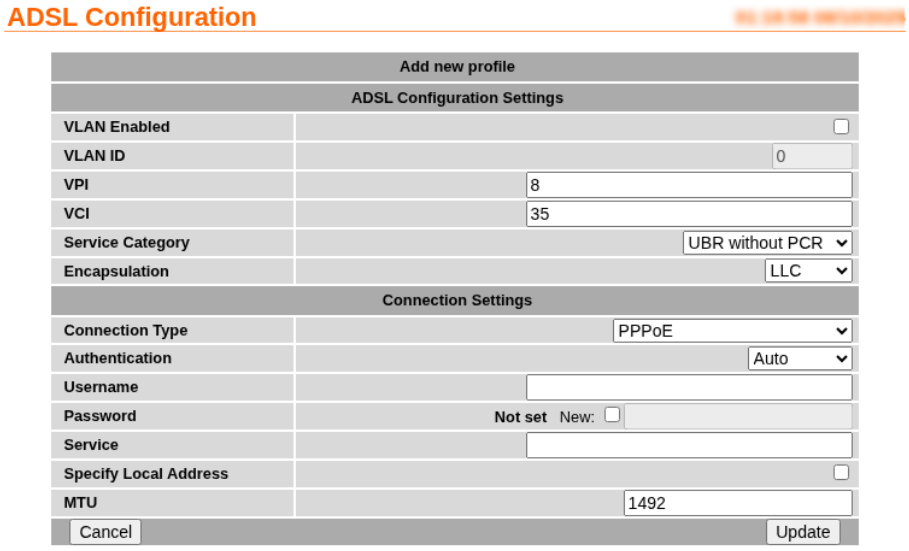


Fig. 7.15: Add new ADSL profile.

Note

The network provider will specify the required settings for completing a connection profile. The provider may not supply a user-name and password if network authentication is not required. In this case set the **Authentication** to **None**.

The first section relates to the settings for the DSL connection, and is common to all connection types. The options are:

ADSL Configuration Settings

VLAN Enabled
Check to enable VLAN over the DSL interface.

VLAN ID
Enter the VLAN ID for use over the DSL interface.

VPI
Virtual Path Identifier.

VCI
Virtual Circuit Identifier.

Service Category
The ATM forum-defined service category. Options:

UBR without PCR
Unspecified Bit Rate without Peak Cell Rate (PCR)

UBR with PCR
Unspecified Bit Rate with Peak Cell Rate (PCR)

PCR
Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

CBR
Constant Bit Rate, for ATM virtual circuits requiring a static amount of bandwidth.

PCR
Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

Non Realtime VBR
Non-Real-Time Variable Bit Rate (nrt-VBR)

PCR
Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

SCR
Sustainable Cell Rate. A calculation of the average allowable, long-term cell transfer rate on a specific connection.

MBS
Maximum Burst Size. The maximum allowable burst size of cells that can be transmitted contiguously on a connection.

Realtime VBR
Real-Time Variable Bit Rate (rt-VBR)

PCR
Peak Cell Rate. The maximum allowable rate at which cells can be transported along a connection.

SCR
Sustainable Cell Rate. A calculation of the average allowable, long-term cell transfer rate on a specific connection.

MBS
Maximum Burst Size. The maximum allowable burst size of cells that can be transmitted contiguously on a connection.

Encapsulation
Select the mechanism for identifying the protocol carried in ATM Adaptation Layer 5 (AAL5) frames. Options:

LLC
Logical Link Control.

VC MUX
Virtual Circuit Multiplexing.

The options within the first section listed under the titled Add new profile will changed depending on the selected connection type. The first step is to select the connection type from the drop-down list, the options are:

Connection Type
The ADSL connection type is selected from the drop-down list. Once selected the options will be changed to those relevant for the selected connection type.

PPPoA
Point to Point Protocol over Asynchronous Transfer Mode (ATM) is a method of transporting PPP frames over ATM.

PPPoE
Point to Point Protocol over Ethernet is a method of encapsulating PPP frames within Ethernet frames.

MAC Encapsulated Routing
Is a method of encapsulating Ethernet frames for transfer over ATM.

IPoE
Internet Protocol over Ethernet is a method of encapsulating IP datagrams with Ethernet frames without using PPPoE.

Bridged
Creates a direct connection between the LAN (Ethernet) interface and the DSL interface.

Once the connection type has been selected refer to the appropriate section below for the relevant settings.

Connection Type PPPoA

When Point to Point Protocol over ATM (PPPoA) is selected as the connection type the PPPoE options will be shown, refer to Fig. 7.16 for details.

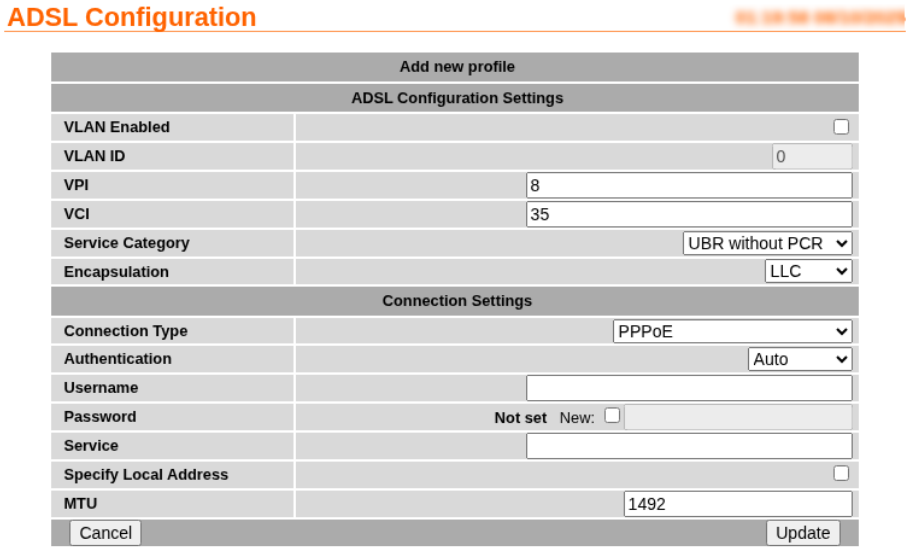


Fig. 7.16: Add new ADSL profile with connection type PPPoA.

Connection Type:

PPPoA
The PPPoA otpion is selected.

Authentication
For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None
No authentication is performed.

PAP
The Password Authentication Protocol is used.

CHAP
The Challenge-Handshake Authentication Protocol is used.

Auto(Default)
The authentication protocol is automatically determined.

MS-Chap
The Microsoft version of the Challenge-Handshake Authentication Protocol (CHAP) is used.

Username
For connections where the Authentication is not set to None, this is the user-name the modem will use to authenticate.

Password
For connections where the Authentication is not set to None, this is the password the modem will use to authenticate. In order to set a password click the check box marked New then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

Service
The service string.

MTU
Setting for the Maximum Transmission Unit of the DSL interface.

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type PPPoE

When Point to Point Protocol over Ethernet (PPPoE) is selected as the connection type the PPPoE options will be shown, refer to Fig. 7.17 for details.

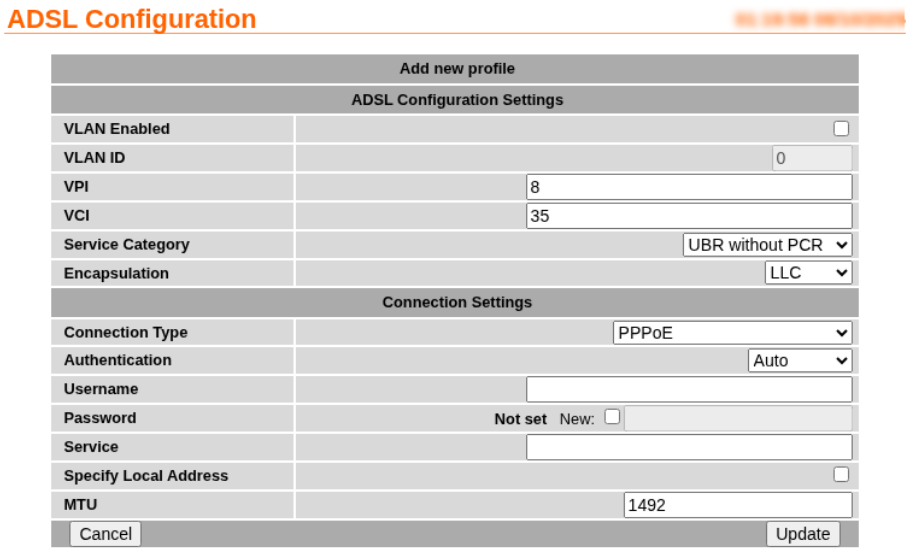


Fig. 7.17: Add new ADSL profile with connection type PPPoE.

Connection Type:

PPPoE
The PPPoE option is selected.

Authentication
For connections requiring a user-name and password to connect, this field sets the authentication protocol used:

None
No authentication is performed.

PAP
The Password Authentication Protocol is used.

CHAP
The Challenge-Handshake Authentication Protocol is used.

Auto (Default)
The authentication protocol is automatically determined.

MS-Chap
The Microsoft version of the Challenge-Handshake Authentication Protocol (CHAP) is used.

Username
For connections where the Authentication is not set to None, this is the user-name the modem will use to authenticate.

Password
For connections where the Authentication is not set to None, this is the password the modem will use to authenticate. In order to set a password click the check box marked New then enter the password in the adjacent text field. The password is visible as it is being typed so that it can be checked for errors prior to being set. Once set the password will no longer be visible.

Service
The service string.

MTU
Setting for the Maximum Transmission Unit of the DSL interface.

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type MER

When Point to MAC Encapsulated Routing (MER) is selected as the connection type the MER options will be shown, refer to Fig. 7.18 for details.

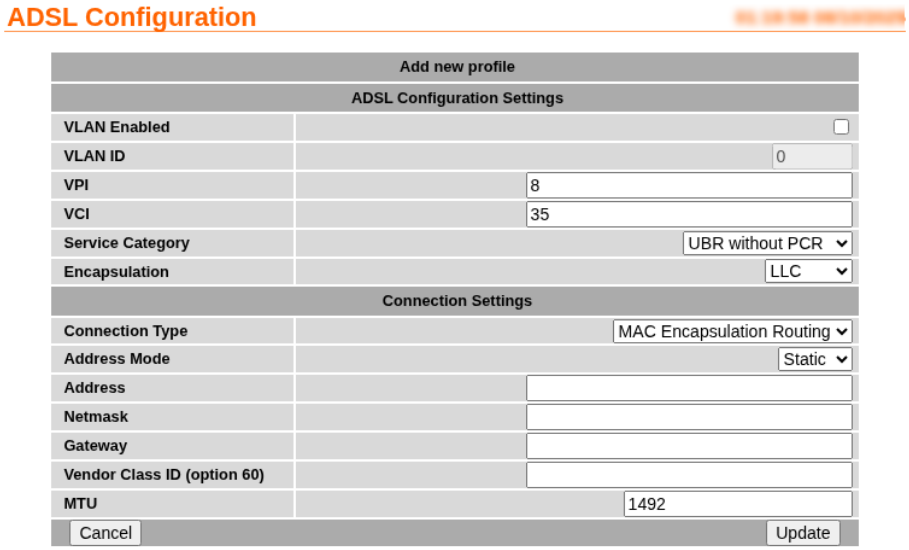


Fig. 7.18: Add new ADSL profile with connection type MAC Encapsulation Routing.

Connection Type

MAC Encapsulation Routing (MER):
The MER option is selected.

Address Mode:

Static
Set a static address IP address for the DSL interface:

Address
The IP address for the interface.

Netmask
The netmask for the interface.

Gateway
The gateway address for the interface.

DHCP
The IP address settings for the interface will be set dynamically.

Vendor Class ID (option 60)
Optional field for specifying a vendor class identifier string. This DHCP option is used to identify the type of device to the DHCP server, which may provide device-specific configuration parameters. Leave blank if not required by the network provider.

MTU
Setting for the Maximum Transmission Unit of the DSL interface.

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type IPoA

When Internet Protocol over ATM (IPoA) is selected as the connection type the IPoA options will be shown, refer to Fig. 7.19 for details.

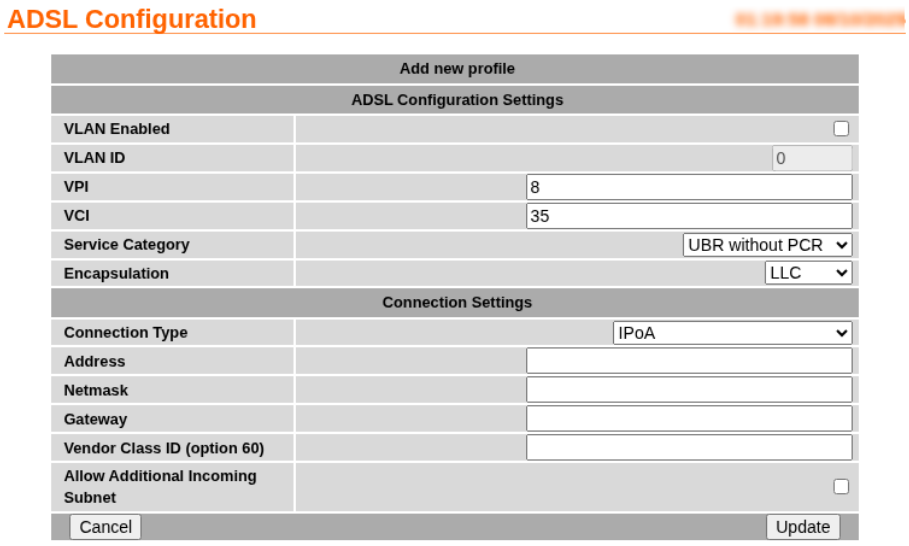


Fig. 7.19: Add new ADSL profile with connection type IPoA.

Connection Type

IPoA:
The IPoA option is selected.

Address
The IP address for the DSL interface.

Netmask
The netmask for the DSL interface.

Gateway
The gateway address for the DSL interface.

Once the profile has been entered click the Update button to save and commit changes. Click the Cancel button to abort adding the new profile.

Connection Type Bridged

When Bridged is selected as the connection type there are no configurations settings required, refer to Fig. 7.20 for details.

Connection Type

Bridged
ADSL Bridged mode is selected.

No settings required for bridged mode.

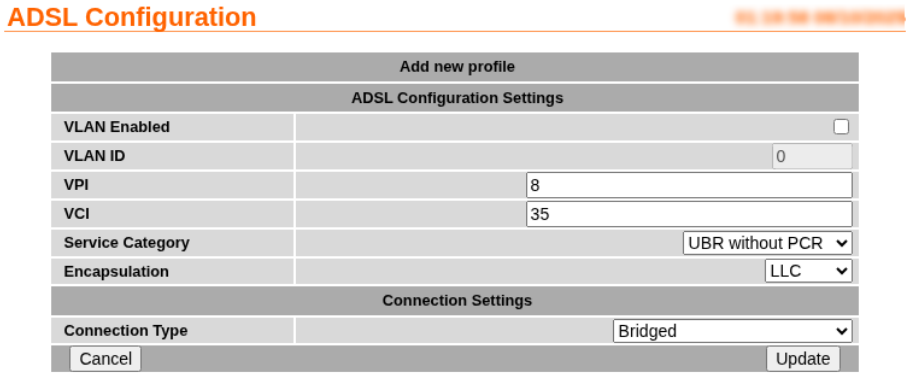


Fig. 7.20: Add new ADSL profile with connection type bridged.

7.3.3 Example of Adding an ADSL Profile

In this example a profile will be added with the following details:

ADSL Configuration Settings:

VLAN Enabled
Unchecked (disabled)

VPI
8

VCI
35

Service Category
UBR without PCR

Encapsulation
LLC

ADSL Connection Settings:

Connection Type
MAC Encapsulation Routing (MER)

Address Mode
Static :Address: 10.10.80.2 :Netmask: 255.255.255.0 :Gateway: 10.10.80.1

Vendor Class ID (option 60)
(left blank)

MTU
1492

To access the ADSL configuration, select *DSL → ADSL Mode* from the menu, a page as shown in Fig. 7.14 will be displayed. Assuming no profiles have been configured the profiles section of the page will be as shown in Fig. 7.21.

To add an ADSL profile click the Add new profile button, the Add New Profile page as shown and the details as listed above can be entered as shown in Fig. 7.22.

Once the profile has been entered click the Update button to save and commit changes.

The main ADSL page will be shown again, and the new profile will be included in the profiles list, as shown in Fig. 7.23.

Within the Connection Configuration section the profile should be selected as the active profile. To enable the connection change the Connection Mode from Disabled to Always connect.

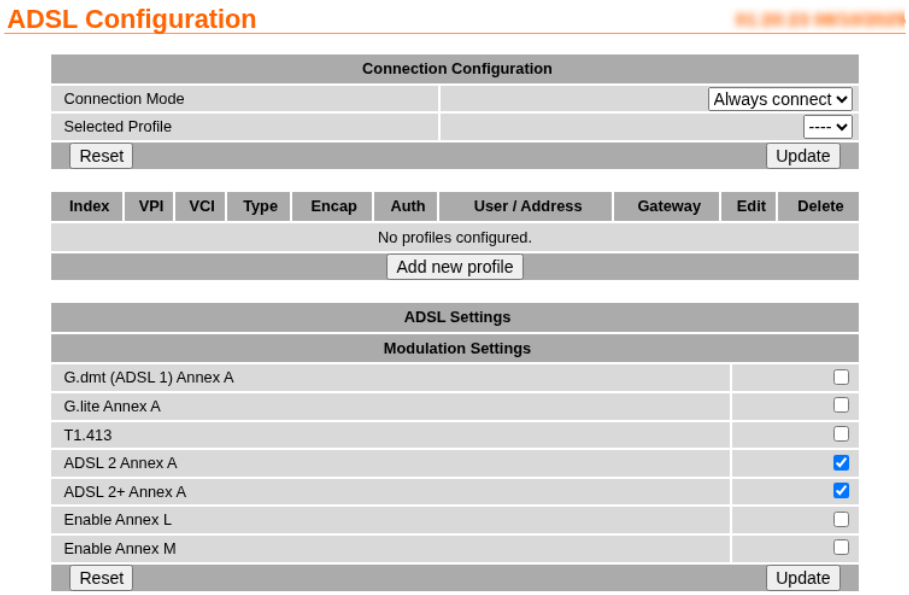


Fig. 7.21: ADSL with no profiles.

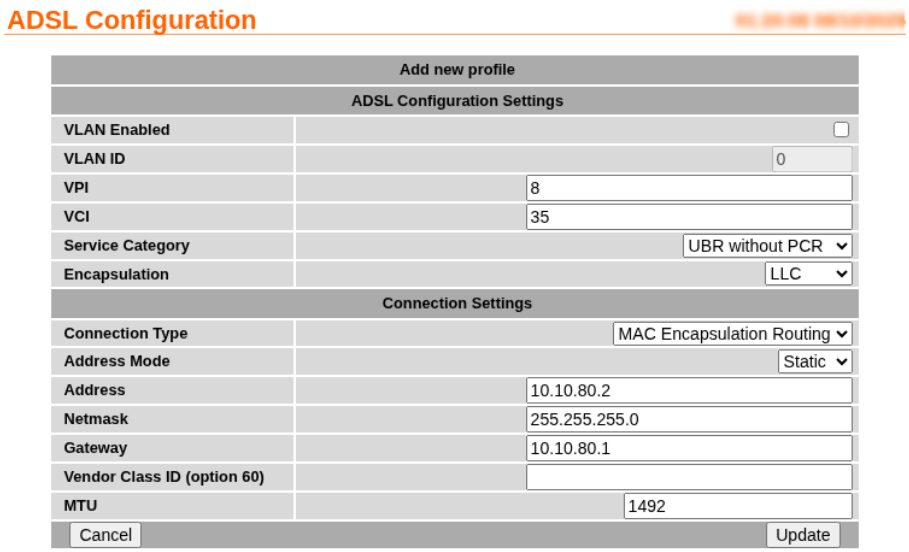


Fig. 7.22: Example of adding an ADSL profile configuration.

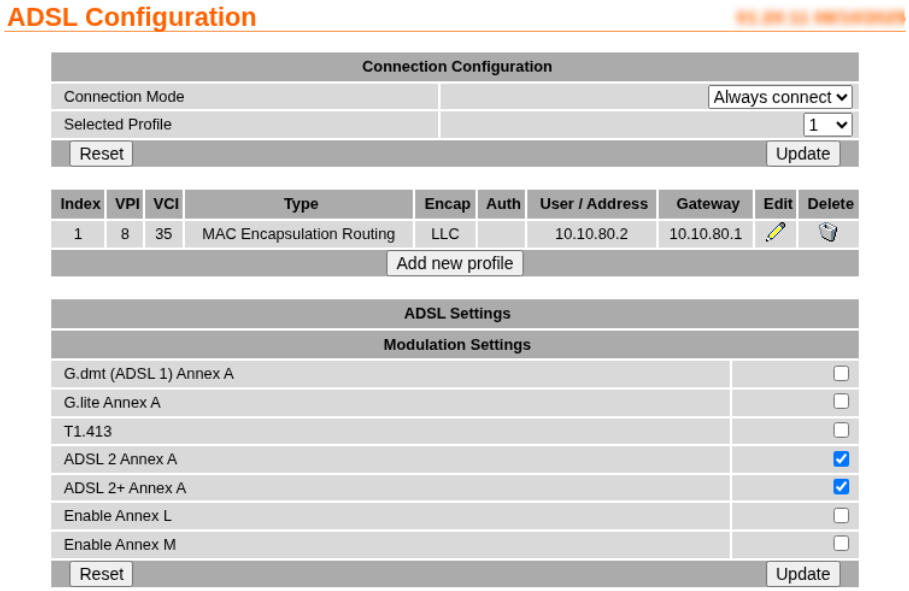


Fig. 7.23: Main ADSL page with newly added profile.

7.3.4 Example of Editing an ADSL Profile

To edit an existing profile click on the  icon located in the **Edit** column for the profile to be edited. A page similar to add profile page, which includes the details for the profile will be displayed.

The edit profile page for the profile entered in the example above are shown in Fig. 7.24.

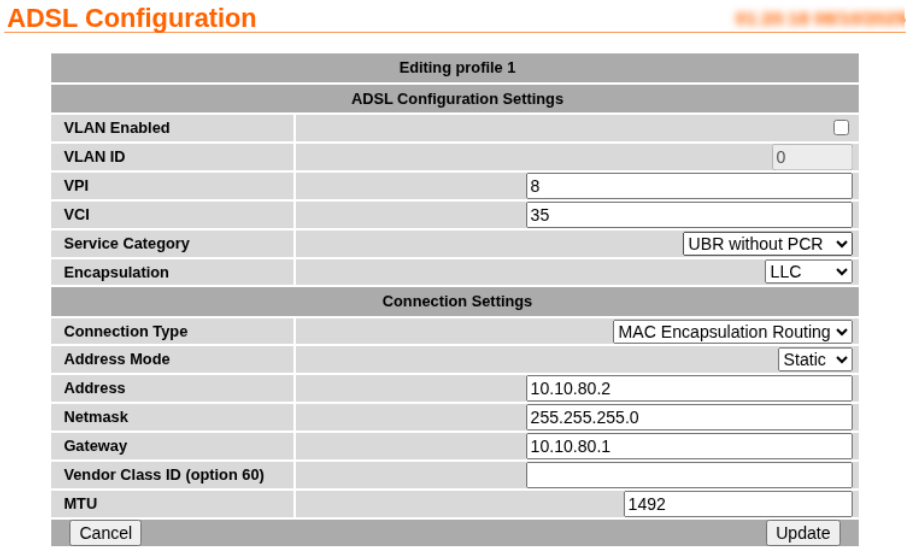


Fig. 7.24: Edit an ADSL profile example.

Once the profile has been entered click the Update button to save and commit changes. To abort the changes and leave the profile unchanged click the Cancel button.

7.3.5 Example of Deleting an ADSL Profile

A profile can be deleted by clicking the icon located in the Delete column for the profile to be deleted. A dialogue box will shown requesting confirmation of the deletion, Click the OK button to proceed with the deletion or click the Cancel button to abort the deletion. Fig. 7.25 illustrations the deleting a profile entered in the example above.

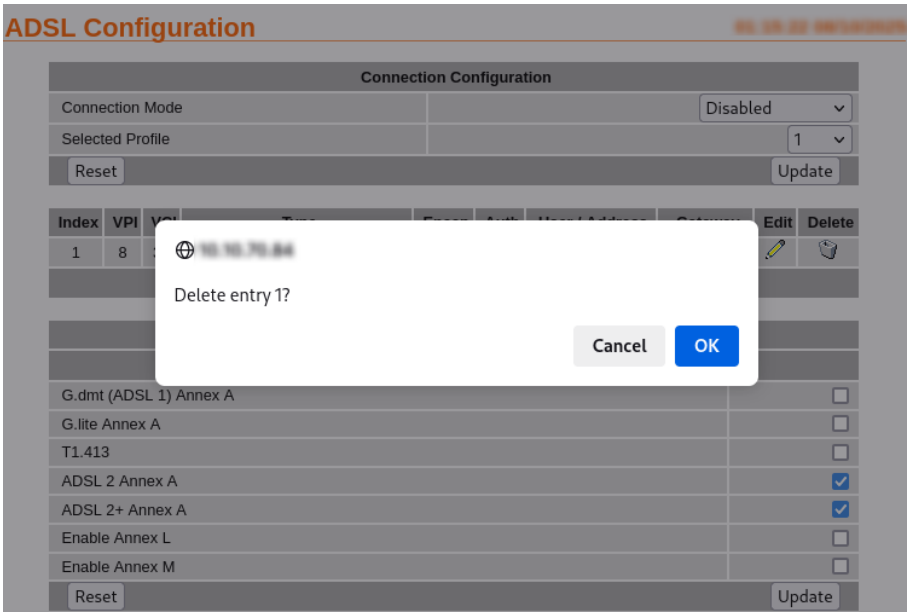


Fig. 7.25: Deleting an ADSL profile.

After confirming the deletion of the profile the main ADSL will be shown and will be similar Fig. 7.26.

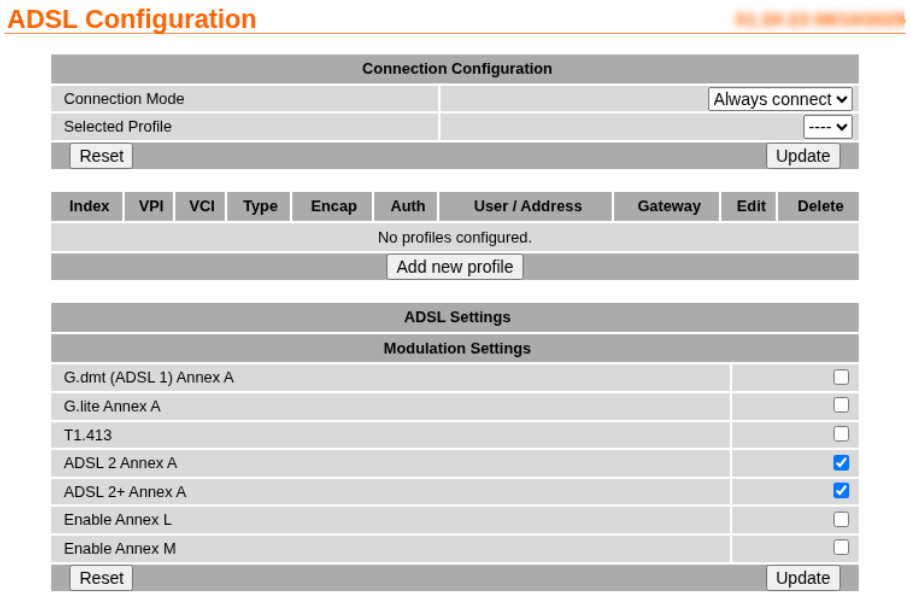


Fig. 7.26: Profile list after deleting the ADSL profile.

7.4 Connection Status

To check the status of the connection select *Status → DSL* from the menu, the DSL Status page will be shown similar to that shown in Fig. 7.27. The Network Status reports on the DSL Synchronisation status, once the connected has synced it will report Up. The connection Status reports on the packet or data connection status, once established this will report Up. For full details on the DSL status page including the Advance Status refer to *DSL Interface Status* in the *Status* chapter.

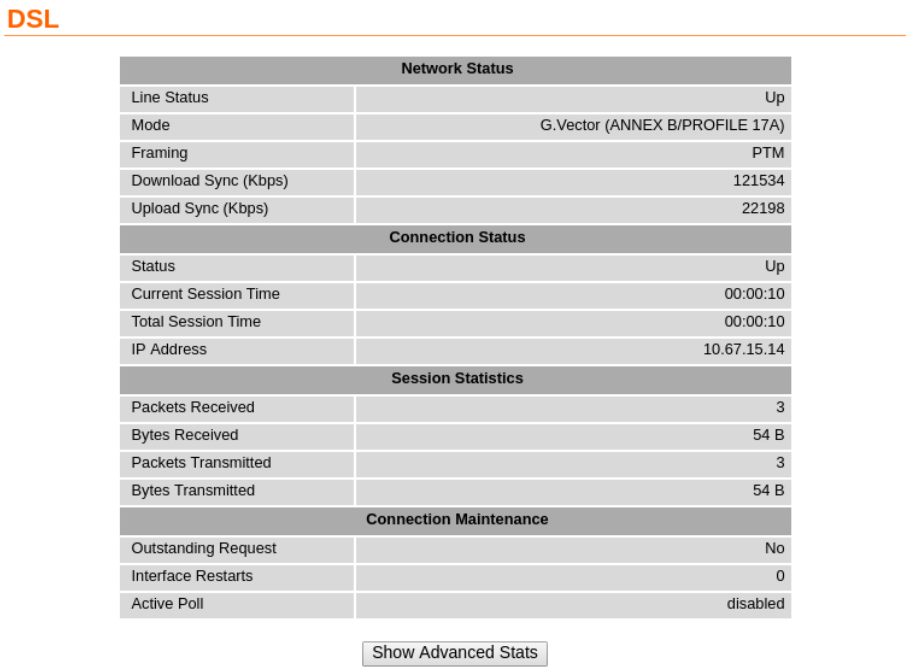


Fig. 7.27: DSL Status page.

With the DSL connection established the Status Alarms page should now indicate no faults as shown in Fig. 7.28.

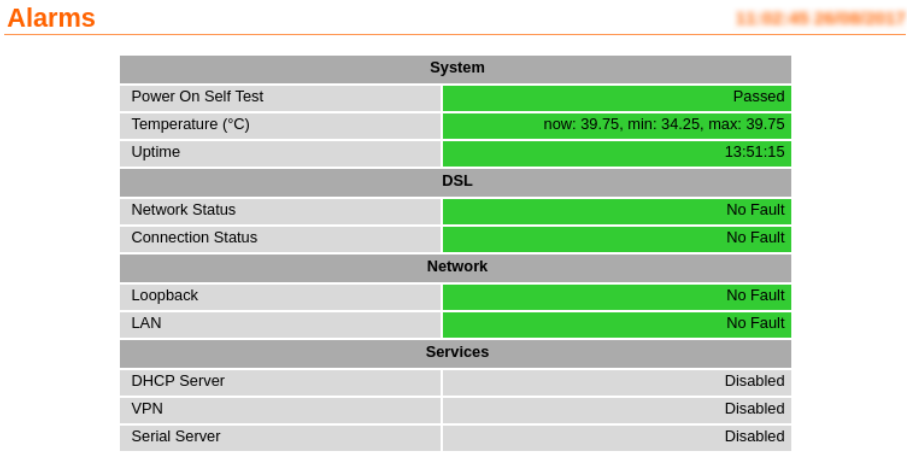


Fig. 7.28: Status Alarms page.

7.5 Connection Management

The purpose of connection management is to create and maintain reliable connections that can detect errors and recover as quickly as possible. The connection management is divided in two areas:

Connection establishment
: Determines how the modem manages the establishment of a connection to the network.

Connection Maintenance
Determines how the modem manages the connection to the network once established.

To access the connection management options, select *DSL → Connection Management* from the menu. The connection management page as shown in Fig. 7.29 will be displayed.

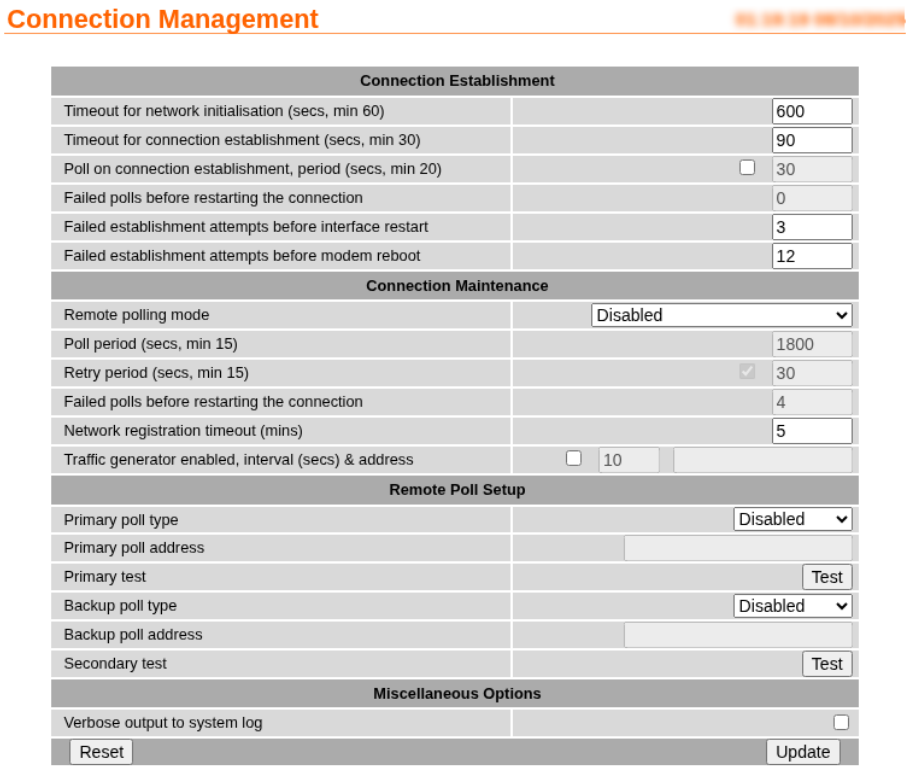


Fig. 7.29: DSL connection management.

7.5.1 Connection Establishment

The connection establishment options are used to set the parameters for initial connection to a provider's DSL network. The options are:

Timeout for network initialisation
Specify the maximum time in seconds to allow for a network initialisation. The minimum value accepted is 60 Seconds, the default value is 120 seconds.

Timeout for connection establishment
Specify the maximum time in seconds to allow for a connection to be established. The minimum value accepted is 30 Seconds, the default value is 45 seconds.

Poll on connection establishment
Check to enable and specify the poll re-try period, the minimum value is 20 seconds. If enabled a remote poll will be completed before the connection is considered successful. The purpose of this option is to ensure that not only has a network connection been established but also that end-to-end connectivity exists. The modem does this by polling a remote server using ICMP (Ping) or a TCP socket connection. Should the poll fail, the modem retries at the specified interval for the number of polls specified in **Failed polls before restarting the connection**. If this option is enabled then the **Remote Poll Setup** must be enabled and configured correctly.

Failed polls before restarting the connection
Set the number of failed polls before the connection is considered to have failed to establish. A value of 0 disables poll on connection establishment. This option is only available when **Poll on connection establishment** enabled.

Failed establishment attempts before interface restart
Specify the number of failed connection attempts before restarting the DSL interface. Set this value to 0 to

disable.

Failed establishment attempts before modem reboot
Specify the number of failed connection attempts before re-booting. Set this value to 0 to disable.

7.5.2 Connection Maintenance

The connection maintenance refers to the tests employed to determine if a valid network connection is available. Should the connection maintenance test fail then attempts will be made to re-establish the connection.

The following options control connection maintenance:

Remote polling mode:
Specify the connection maintenance operating mode. Four modes are supported:

Disabled
Connection maintenance is disabled. (Default)

Poll at fixed interval
Poll the servers specified in the **Remote Poll Setup** at the interval specified.

Poll if Rx idle for interval
Only poll the servers specified in the Remote Poll Setup when no data has been received from the DSL interface for the specified interval.

Reconnect if Rx idle for interval
Monitor the receive data and reconnect if no data has been received by the DSL interface for the specified interval. This mode is a good choice for configurations that already employ polling traffic, such as when using the SSL VPN or IPsec VPN with dead peer detection.

Poll period
Specify the time interval in seconds between polls. Minimum value of 15 seconds.

Retry period
Specify the time in seconds to retry the poll after a failed poll. Minimum value of 15 seconds.

Failed polls before restarting connection
Specify the number of failed polls to declare the link failed and to re-start the establishment process.

Network registration timeout
Specify the time in minutes the time-out for network registration attempt after a polling failure.

Traffic generator enabled, interval & address
Check to enable the traffic generator, and specify the time interval between data packets and the address to which to send the packets. The traffic generator is used to generate transmit data, it sends a data packet at the specified interval without expecting a response.

7.5.3 Remote Poll Setup

The remote poll set-up is used to specify the poll type to use and the address of the server to poll. A primary and backup server may be specified. The backup server will be used if the primary server cannot be contacted. The options for each poll are:

Primary Poll type
Specify the poll type. The options are:

Disabled
The poll is disabled.

Ping (ICMP)
Ping the specified address.

TCP Socket
Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Primary Poll address
Specify the address of the primary server to poll. The format used depends on the poll type:

Ping (ICMP)
Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket
Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Primary test
Click the test button to test the poll.

Backup Poll type:
Specify the poll type. The options are:

Disabled
The poll is disabled.

Ping (ICMP)
Ping the specified address.

TCP Socket
Establish a TCP socket to the specified address and port number. The connection will be terminated as soon as successfully opened.

Backup Poll address
Specify the address of the primary server to poll. The format used depends on the poll type:

Ping (ICMP)
Enter an IP address or host-name, eg 192.168.1.1 or www.exampledomain.com

TCP Socket
Enter an IP address or host-name followed by a colon and the TCP port number, for example 192.168.1.1:80

Secondary test
Click the test button to test the poll.

7.5.4 Miscellaneous Options

Verbose output to system log
Check to enable sending of verbose connection information to the system log. As the size of the system log is limited, this option should only be enabled if connection problems are experienced.

Click the Reset button to revert to the original settings. Click the Update button to save and commit changes.

CHAPTER

EIGHT

NETWORK

This section describes the configuration of the network and LAN settings. This includes setting the IP Address of the Ethernet ports, configuring the DHCP server and the DNS settings. The main Network configuration page is accessed by clicking the Network tab, a page similar to that shown in Fig. 8.1 will be shown.

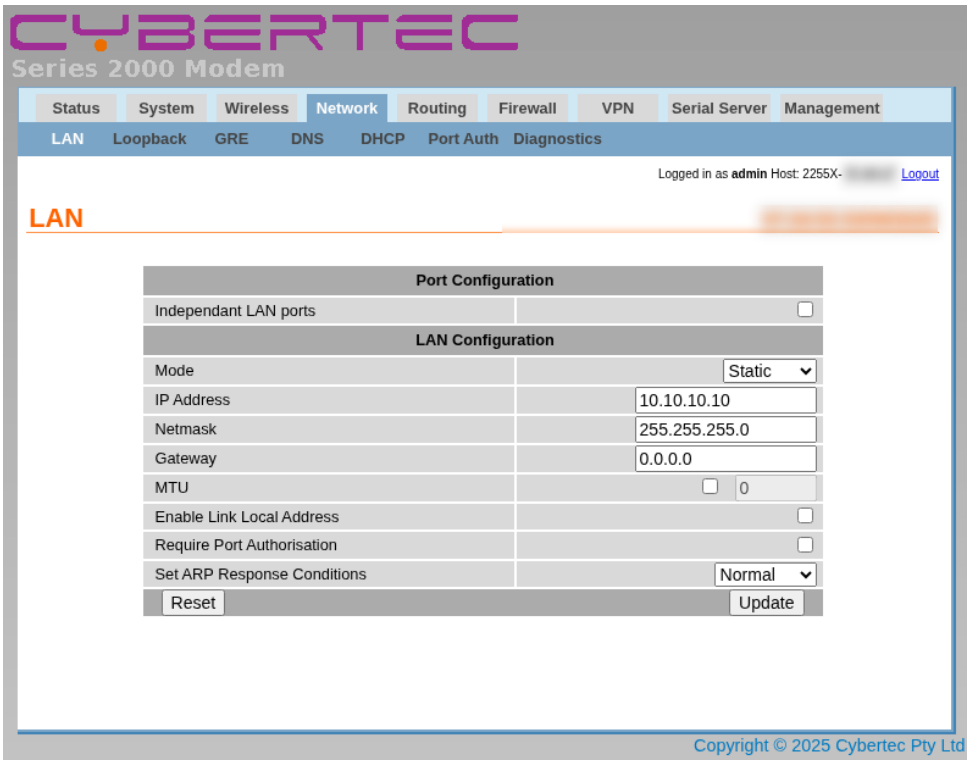


Fig. 8.1: Main Network settings page.

8.1 LAN

The LAN Interface refers to the Ethernet ports of the unit. To access the LAN Interface settings select *Network* → *LAN*. Fig. 8.2 is an example of the LAN settings page.

8.1.1 Port Configuration

The unit has two Ethernet ports which can be configured in two modes:

Bridge Mode (LAN Switch)
: Both ports operate as a single switched network, sharing the same IP configuration.

Independent Mode
: Each port operates independently with separate IP configurations.

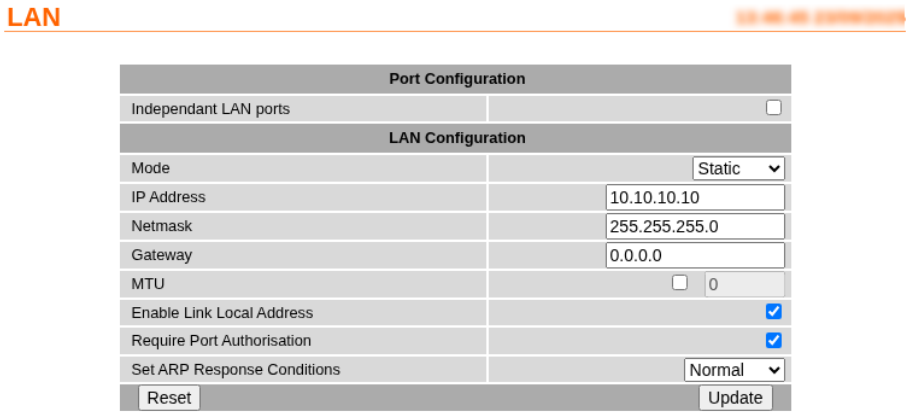


Fig. 8.2: LAN Interface configuration.

To enable independent port operation, check the **Independent LAN Ports** checkbox. When unchecked, the ports operate in bridge mode as a single LAN switch.

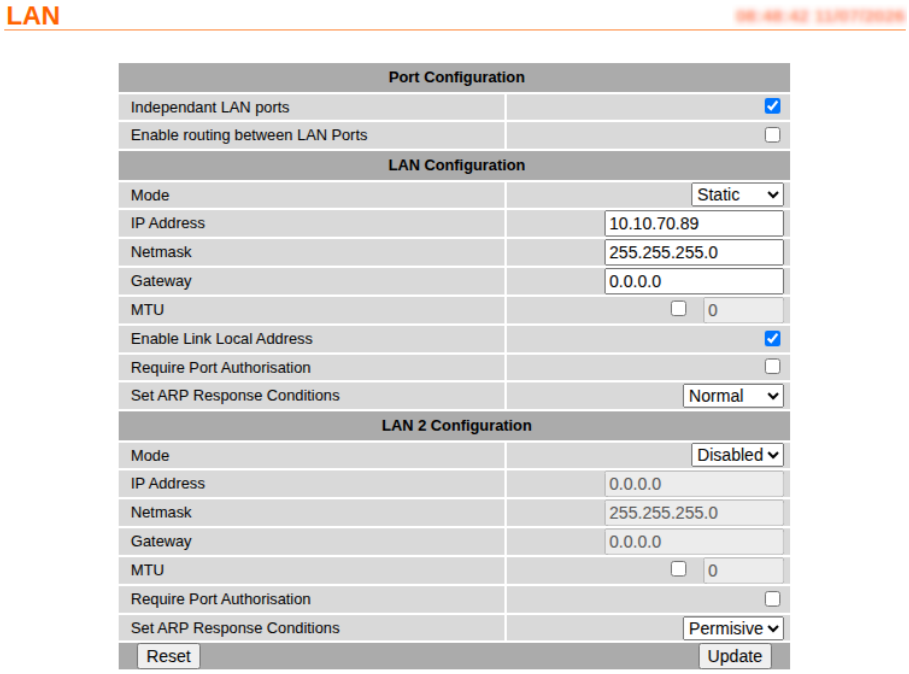


Fig. 8.3: LAN Interface configuration for Independent LAN ports.

Enable routing between LAN Ports
: This option is only available when Independent LAN Ports has been enabled. When checked this option allows IP routing between the LAN interfaces. When unchecked the sub-nets on each LAN port are isolated and LAyer 3 traffic will only be forwarded if explicit routing rules are configured.

8.1.2 LAN Configuration

The LAN configuration options are the same for both LAN ports.

Mode
: Select the IP address assignment mode. Options include:

  Disabled
  : Disable the LAN interface

Static
Manually configure IP address, netmask, and gateway

DHCP
Automatically obtain network settings from a DHCP server

Automatically add DNS obtained via DHCP
Only available when mode set to DHCP. When checked, DNS server addresses received via DHCP on the LAN interface will be added to the system DNS configuration.

IP Address
Enter the IP address for the LAN interface when using Static mode.

Netmask
Enter the subnet mask for the LAN interface when using Static mode.

Gateway
Enter the default gateway address when using Static mode.

MTU
Specify the Maximum Transmission Unit size for the LAN interface. Leave blank to use the default MTU size.

> **Note**
>
> The Maximum Transmission Unit (MTU) for Ethernet II framing is 1500. This is standard framing used by most IP over Ethernet implementations. For this reason it is recommended that this value not be changed from the default value of 1500 except where the sub-net differs from standard.
>
> If uncertain do not change the MTU value from the default of 1500.

Enable Link Local Address
Check to enable automatic Link Local address assignment (169.254.x.x address range) when no other IP configuration is available.

Require Port Authorisation
Refer to **Port Authentication**.

Set ARP Response Conditions
Configure when the device responds to ARP requests:

Permissive
Respond to all ARP requests by default and only ignore requests from known IP addresses

Normal
Standard ARP response behaviour.

Strict
Respond only to ARP requests from known IP addresses

Once any changes have been made to the configuration click the Update button to save the changes.

8.1.3 Changing the IP settings of the LAN Interface

The network settings are contained in the **LAN Configuration** table (as shown in Fig. 8.2). To change the IP settings:

1. Ensure that **Mode** is set to **Static**.
2. Enter the new IP address for the LAN interface in the **IP Address** box.
3. Enter the new netmask in the **Netmask** box.
4. Click the Update button to save and commit changes.

5. **A redirect message will appear in the browser similar to that shown in** Fig. 8.4, the browser will then be directed to the new IP address and the *Network → LAN* will be shown.

Fig. 8.4: LAN Interface redirect message.

Note

If the redirect does not happen automatically, enter the new IP address into the web browser, it will also be necessary to login again due to the IP address change. For details on accessing the web pages and logging into the unit refer to chapter **Accessing the Web Interface**.

8.1.4 Disabling the LAN Interface

By default the LAN interface is enabled, however, for installations where the LAN ports are not required once initial configuration is complete, the ports can be disabled.

Warning

If the LAN ports are disabled then access to the web configuration pages will only be available via the wireless interface (if the firewall settings allow access to the web server, for details on the Firewall configuration refer to chapter **Firewall**).

To disable the LAN Interface:

1. Set **Mode** to **Disabled** in the **LAN Configuration** table.
2. **A warning dialogue box will be displayed (similar to** Fig. 8.5), warning that once the change has been committed the LAN interface will not be accessible.
3. Click the OK button.
4. Click the Update button to save and commit changes.

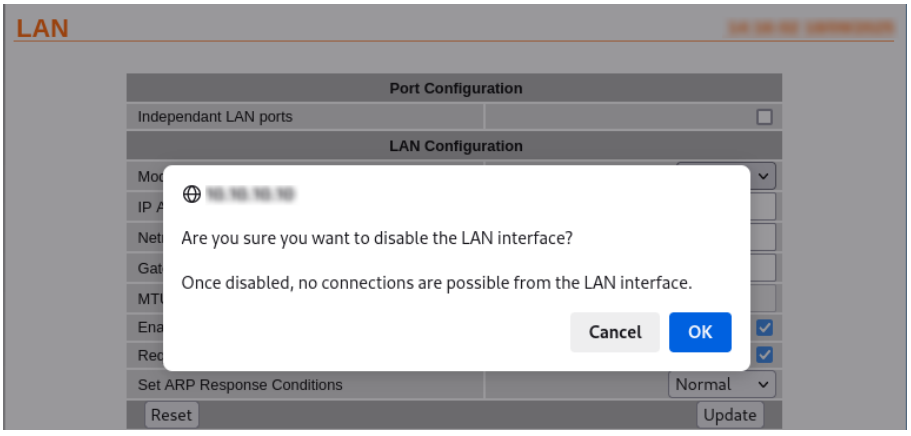


Fig. 8.5: LAN Interface disable warning.

The LAN interface will now be disabled.

Note

To re-enable the LAN ports without accessing the web interface, it will be necessary to perform a factory reset of the unit. This will clear all the configuration settings to the factory default settings and the LAN ports will be enabled. Refer to the manual for the model being configured for details on how to perform a factory reset.

8.2 DHCP

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides devices connected on a Local Area Network (LAN) with an IP address and other related configuration information such as the subnet mask and default gateway.

To access the DHCP server configuration, select *Network* → *DHCP*. The DHCP configuration page is shown in Fig. 8.6.

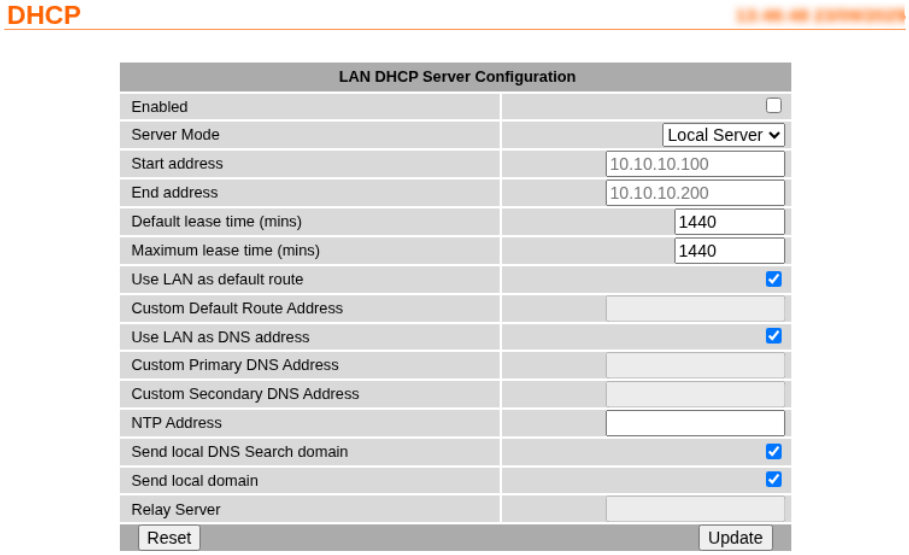


Fig. 8.6: DHCP server configuration.

8.2.1 LAN DHCP Server Configuration

The default configuration of the DHCP server will serve IP addresses in the range 10.10.10.100 through 10.10.10.200 to requesting devices connected to the LAN interface. If the default IP address of the unit hasn't been changed this may be a suitable configuration and only enabling DHCP is required.

The configuration options available are:

Enabled
Set the check-box to enable the DHCP server.

Server Mode
Select the DHCP server operation mode:

Local Server
The unit acts as a DHCP server, providing IP addresses from the configured pool.

Relay
The unit forwards DHCP requests to another DHCP server on the network.

Start address
The first IP address in the pool allocated by the DHCP server. This address must be on the same subnet as the LAN IP address.

End address
The last IP address in the pool allocated by the DHCP server. This address must be on the same subnet as

the LAN IP address and greater than the Start address.

Default lease time (mins)
This field configures the default lease time given to clients. The value entered is in minutes. Default: 1440 (24 hours)

Maximum lease time (mins)
This field configures the maximum lease time given to clients. The value entered is in minutes. Default: 1440 (24 hours)

Use LAN as default route
When checked, the DHCP server will provide the LAN interface IP address as the default gateway to DHCP clients.

Custom Default Route Address
When "Use LAN as default route" is unchecked, specify a custom gateway address to be provided to DHCP clients.

Use LAN as DNS address
When checked, the DHCP server will provide the LAN interface IP address as the DNS server to DHCP clients.

Custom Primary DNS Address
When "Use LAN as DNS address" is unchecked, specify a custom primary DNS server address to be provided to DHCP clients.

Custom Secondary DNS Address
When "Use LAN as DNS address" is unchecked, specify a custom secondary DNS server address to be provided to DHCP clients.

NTP Address
Specify an NTP (Network Time Protocol) server address to be provided to DHCP clients for time synchronization.

Send local DNS Search domain
When checked, the DHCP server will provide the local DNS search domain to clients, allowing them to resolve local hostnames without fully qualified domain names.

Send local domain
When checked, the DHCP server will provide the local domain name to DHCP clients.

Relay Server
When Server Mode is set to "Relay", specify the IP address of the DHCP server to which requests should be forwarded.

Click the Update button to save and commit changes.

The DHCP server will start and devices may start to request IP addresses. Any DHCP leases granted will be listed on the *Status* → *LAN* page, refer to chapter **Status** for details.

8.3 Loopback Interface

The loopback interface is a virtual interface which means it is an interface not associated with any hardware or network. Once configured the loopback interface address does not change, this is distinct from physical interfaces which could be disabled or the address changed. To access the loopback interface settings select the *Network* → *Loopback* page. The Loopback setting page is shown in Fig. 8.7.

8.3.1 Loopback Interface Configuration

Enabled
Check to enable the loopback interface.

IP Address
The IP address of the loopback interface.

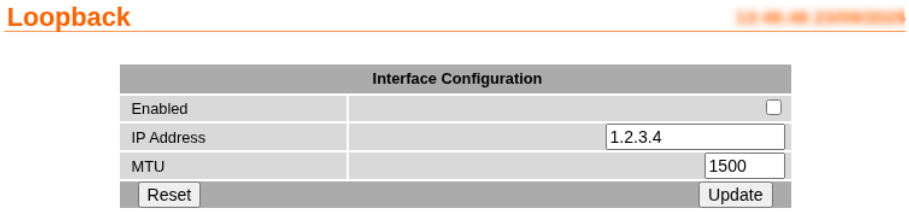


Fig. 8.7: Loopback interface configuration.

MTU
: The Maximum Transmission Unit (MTU) of the loopback interface.

Click the Update button to save and commit changes.

8.3.2 Example Loopback Interface Configuration

An example Loopback interface configuration, with IP address of 10.10.10.123 is shown in Fig. 8.8.

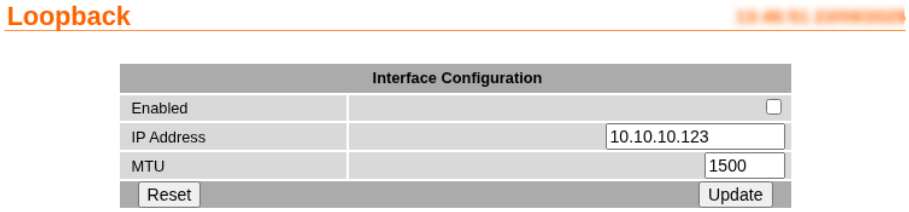


Fig. 8.8: Example Loopback interface configuration.

8.4 Domain Name System (DNS)

The Domain Name System (DNS) is used to resolve domain names to IP addresses. DNS proxy, manual DNS configuration and a dynamic DNS client are all supported. To access the DNS settings select the *Network → DNS* page. The DNS settings page is shown in Fig. 8.9.

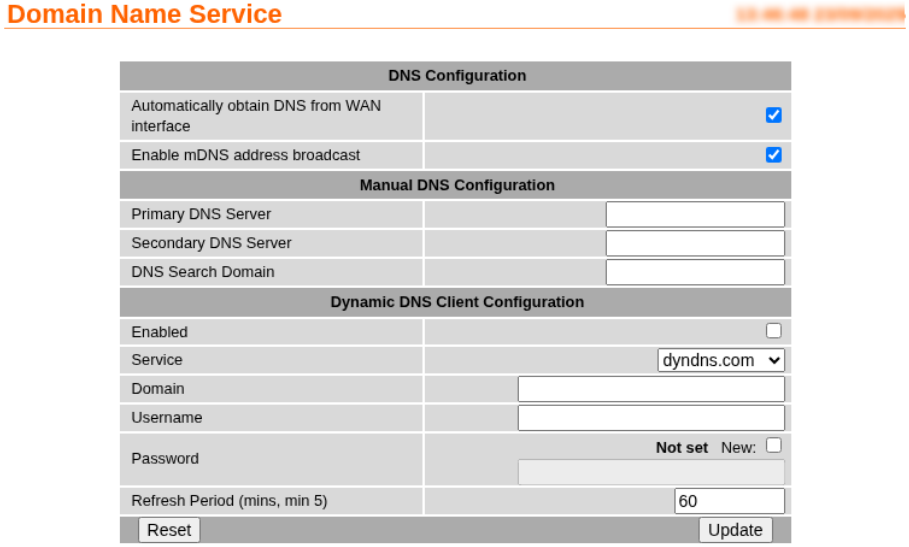


Fig. 8.9: Domain Name Service (DNS) configuration.

8.4.1 DNS Configuration

The **DNS Configuration** section provides options for controlling how the unit obtains and handles DNS settings:

Automatically obtain DNS from WAN interface
When checked, the unit will automatically use DNS server addresses provided by the WAN connection, such as from the mobile network.

Enable mDNS address broadcast
When checked, enables multicast DNS (mDNS) address broadcasting, which allows devices on the local network to discover and resolve local services without requiring a traditional DNS server.

8.4.2 DNS Proxy

The Domain Name System (DNS) proxy allows clients to use the unit as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. When a DNS query is resolved by the DNS proxy, the result is stored in the device's DNS cache. The cached result is then used to resolve subsequent queries from the same domain which minimises data over the wireless network and avoids the delay due to network latency.

The cached results have an associated time-to-live (TTL) timer, when the TTL expires the entry will be purged from the cache. The DNS proxy also simplifies configuration of LAN clients, as they only need to configure the IP address of the DNS proxy as the DNS server. If the DHCP server has been enabled (refer to section *DHCP*) then any device that connects to the LAN interface which requests an IP address from the DHCP server will also be given the IP address of the DNS proxy to use as the DNS server.

8.4.3 Manual DNS Configuration

In the majority of cases, the unit will automatically receive DNS server addresses when establishing a network connection over the WAN interface. In the majority of cases this will be the best DNS server to use.

Should it be necessary to override these values and manually enter DNS server addresses, the alternative DNS server addresses can be entered in the **Manual DNS Configuration** table. The configuration options are:

Primary DNS Server
This is the IP address of the first DNS server to be queried. The value entered should be in IPv4 decimal dotted notation.

Secondary DNS Server
This is the IP address of the secondary DNS server to be queried. The value entered should be in IPv4 decimal dotted notation.

DNS Search Domain
This domain will be appended to requests without a domain name. It is useful for resolving client names on the LAN.

Click the Update button to save and commit changes.

8.4.4 Dynamic DNS Client Configuration

Dynamic DNS is a system which allows the domain name data held in a name server to be updated in real time. The most common use for this is in allowing an Internet domain name to be assigned to a device with a dynamic IP address.

If the wireless service the modem connects to allocates the modem a public, dynamic IP address, it may be possible to use a dynamic DNS provider to update the address of the modem in the DNS system. Once this address is registered, other hosts with Internet access can reach the modem at the domain name.

Table 8.1: *Dynamic DNS providers*

Drop-down Option	Provider
dyndns.com	https://www.dyndns.com/
no-ip.com	https://www.noip.com/
zoneedit.com	https://www.zoneedit.com/
easydns.com	https://easydns.com/
duckdns.org | https://www.duckdns.org/	

Note

Not all wireless providers allocate public IP addresses. Addresses in the range 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255 and 192.168.0.0 - 192.168.255.255 are not public addresses and will most likely not be suitable for use with dynamic DNS.

Some wireless providers do not allow inbound connections at all, so even though the dynamic DNS client will connect and register the IP address provided to the unit, all attempts to connect to that IP address will fail.

In order to use the dynamic DNS feature, it is first necessary to register at a dynamic DNS provider. The supported providers are listed in Table 8.1.

Once registration is complete, the fields of the **Dynamic DNS Client Configuration** table must be completed. The fields are explained below.

Enabled
Set this check-box to enable dynamic DNS updating.

Service
Select the appropriate service from the list.

Domain
Enter the name of the domain allocated by the dynamic DNS provider.

Username
Enter the user-name for the account with the dynamic DNS provider.

Password
Enter the password for the account with the dynamic DNS provider. Check "New:" to set a new password, or leave unchecked if password is already configured.

Refresh Period (mins, min 5)
Set the refresh period in minutes for updating the dynamic DNS record. The minimum allowed value is 5 minutes.

Click the Update button to save and commit changes.

Fig. 8.10 shows an example DynDNS configuration.

8.5 Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE) is a tunnelling protocol which can encapsulate a wide variety of network layer protocol packet types within a virtual point-to-point link over an IP network. To access the GRE configuration page select *Network* → *GRE* a page similar to that shown in Fig. 8.11 will be displayed. This page lists all currently configured tunnels.

To add a new GRE tunnel click the Add new tunnel button and a page similar to that shown in Fig. 8.12 will be displayed.

The available options are:

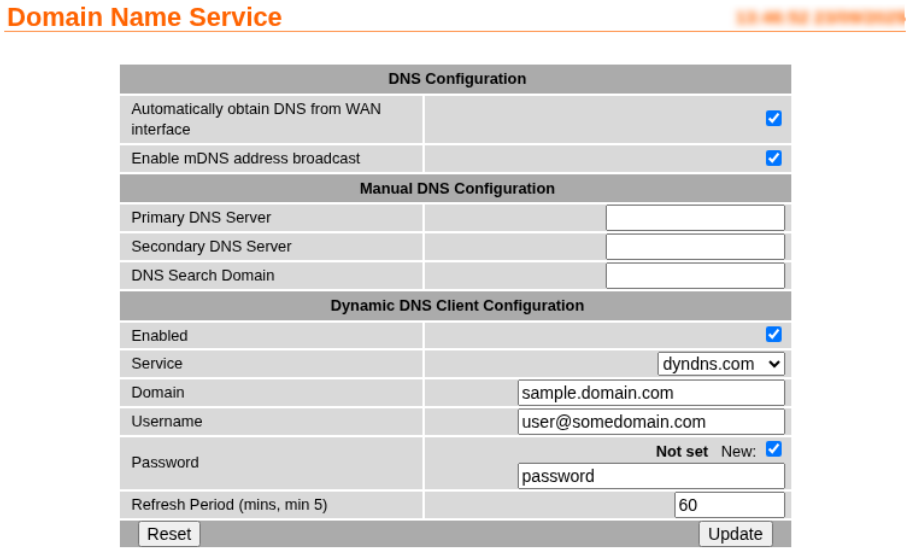


Fig. 8.10: Dynamic DNS Client configuration.

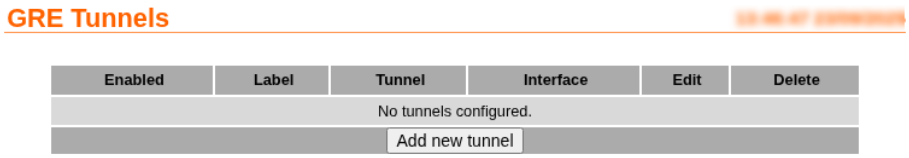


Fig. 8.11: GRE configuration.

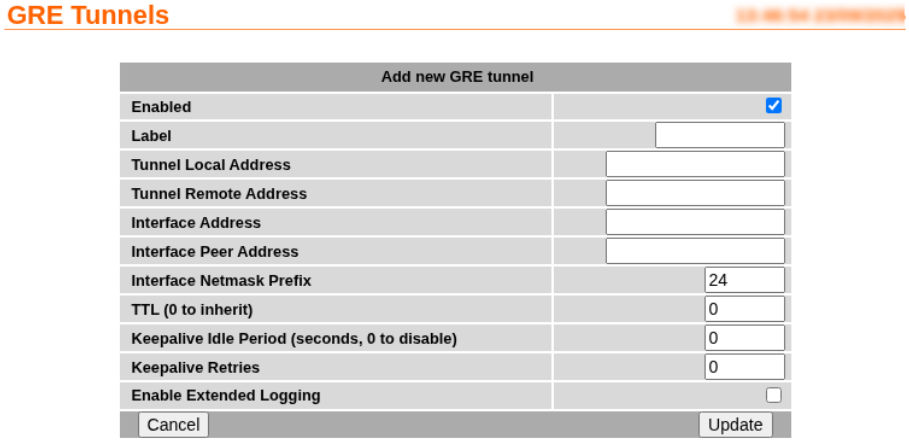


Fig. 8.12: Add a GRE tunnel.

Enabled
Check to enable this particular tunnel.

Label
The name or label associated with the tunnel.

Tunnel Local Address
The local IP address from which the tunnel originates.

Tunnel Remote Address
The remote IP address to which the tunnel connects.

Interface Address
The IP address assigned to the tunnel interface.

Interface Peer Address
The IP address of the remote peer endpoint for the tunnel interface.

Interface Netmask Prefix
The subnet mask prefix length for the tunnel interface (e.g., 24 for /24).

TTL (0 to inherit)
Time To Live value for tunnel packets. Set to 0 to inherit from the encapsulated packets.

Keepalive Idle Period (seconds, 0 to disable)
The time in seconds before sending keepalive packets. Set to 0 to disable keepalive.

Keepalive Retries
The number of keepalive retry attempts before considering the tunnel down.

Enable Extended Logging
Check to enable detailed logging for debugging.

Click the Update button to save and commit changes.

8.6 Port Authentication

Port Authentication provides network access control by requiring devices to authenticate before being granted access to the LAN. This feature implements IEEE 802.1X authentication, allowing only authorized devices to connect to the network. To access the Port Authentication settings select the *Network* → *Port Auth* page. The Port Authentication settings page is shown in Fig. 8.13.

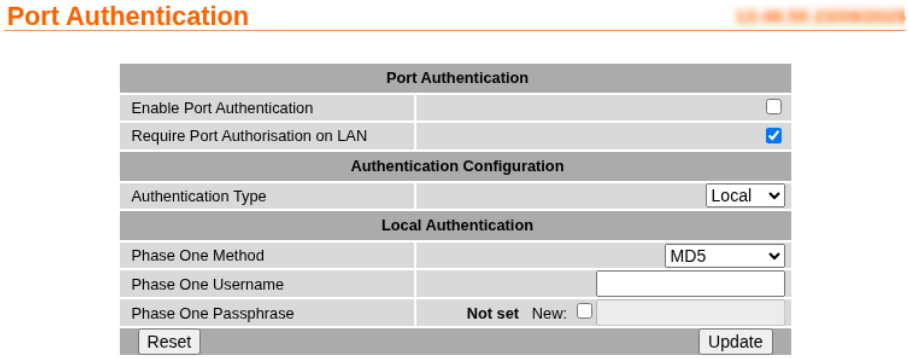


Fig. 8.13: Port Authentication configuration.

8.6.1 Port Authentication Configuration

Enable Port Authentication
Check to enable the port authentication feature on the device.

Require Port Authorisation on LAN
When checked, all devices connecting to the LAN interface must successfully authenticate before being granted network access.

8.6.2 Authentication Configuration

Authentication Type
Select the authentication method:

Local
Use credentials stored locally on the device

Radius
Use an external RADIUS server for authentication

8.6.3 Local Authentication

When Local authentication is selected, the following options are available. The Local authentication configuration is shown in Fig. 8.14.

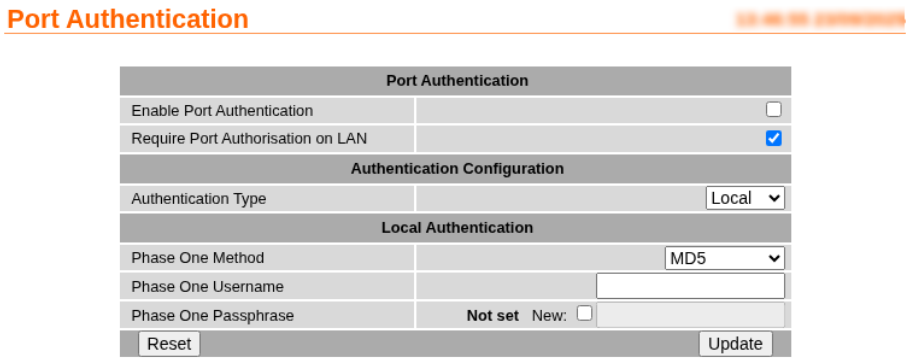


Fig. 8.14: Local Authentication configuration.

Phase One Method
Select the authentication method for the initial phase:

MD5
MD5 Challenge-Response authentication

MSCHAPV2
Microsoft Challenge-Response authentication version 2

Phase One Username
Enter the username for local authentication.

Phase One Passphrase
Enter the passphrase for local authentication. Check "New:" to set a new passphrase, or leave unchecked if passphrase is already configured.

8.6.4 RADIUS Authentication

When RADIUS authentication is selected, the following options are available. The RADIUS authentication configuration is shown in Fig. 8.15.

NAS Identifier
Network Access Server identifier sent to the RADIUS server.

Radius Auth Host
IP address or hostname of the RADIUS authentication server.

Radius Auth Port
Port number for RADIUS authentication (default: 1812).

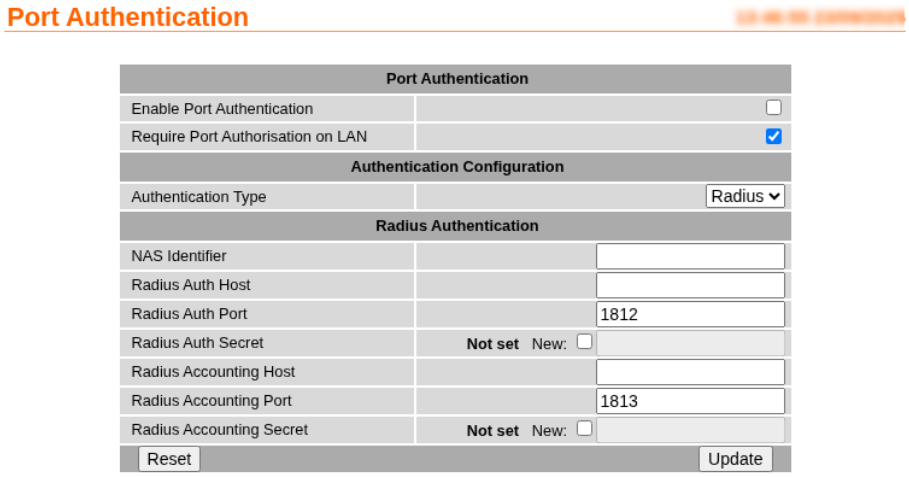


Fig. 8.15: RADIUS Authentication configuration.

Radius Auth Secret
Shared secret for communicating with the RADIUS authentication server. Check "New:" to set a new secret.

Radius Accounting Host
IP address or hostname of the RADIUS accounting server.

Radius Accounting Port:
Port number for RADIUS accounting (default: 1813).

Radius Accounting Secret
Shared secret for communicating with the RADIUS accounting server. Check "New:" to set a new secret.

Click the Update button to save and commit changes.

8.7 Network Diagnostics

Ping and Traceroute are two commonly used tools for analysing packet flows and diagnosing network issues. Ping and traceroute requests can be generated via the web interface. To access the diagnostic tools, select *Network* → *Diagnostics*. Fig. 8.16 illustrates the available options. The top section is used to select the test type and enter the host name or IP address. The results are presented in the box below.

To initiate a test, select Ping or Traceroute as appropriate and enter a host-name or IP address in the Host field. Click the Start button to begin the test. The web page will refresh every 3 seconds until the test completes. A test can be cancelled or the result box cleared by clicking the Cancel button.

Fig. 8.17 is an example of a completed ping test.

8.7.1 Traffic Diagnostics

The Traffic Diagnostics feature provides network packet capture capabilities that can be used to analyze network traffic flows and diagnose communication issues. This tool captures packets from specified network interfaces and protocols, generating pcap-compatible files that can be analyzed using tools like Wireshark.

Interface Selection
Select the network interface from which to capture traffic:

LAN
Capture traffic from the LAN Ethernet interface

Wireless
Capture traffic from the wireless interface (if available)

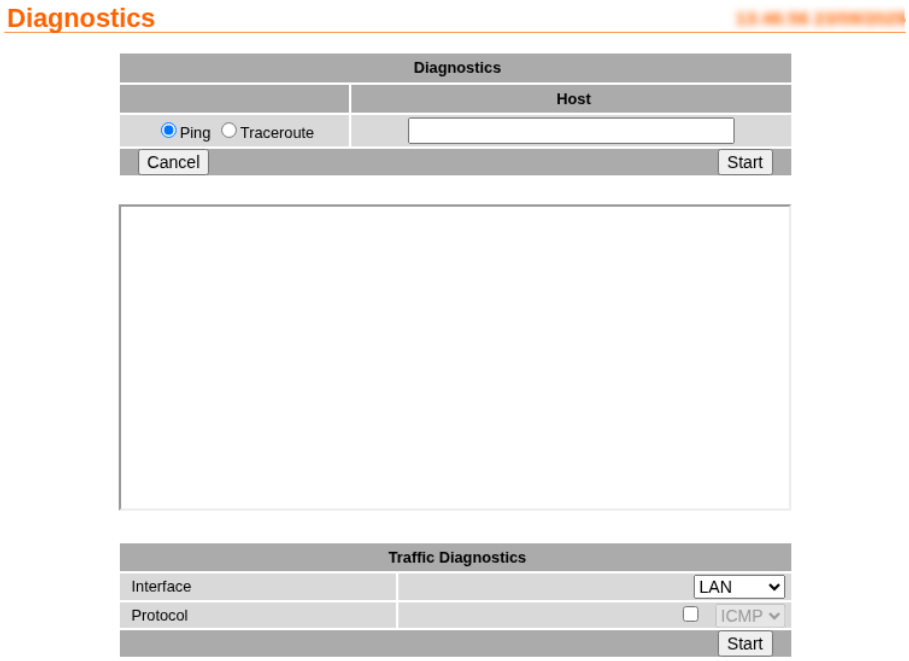


Fig. 8.16: Network diagnostics.

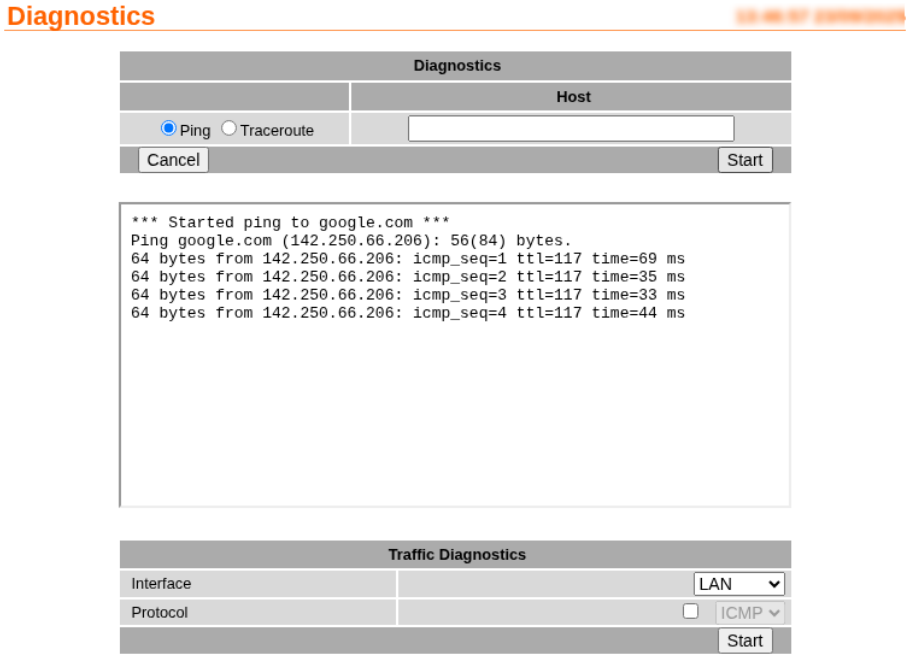


Fig. 8.17: Network diagnostics test.

Protocol Selection
Configure which protocol types to capture:

Protocol Filter
Check the checkbox to enable protocol filtering

Protocol Type
Select from available protocols:

ICMP
Internet Control Message Protocol (ping, error messages)

TCP
Transmission Control Protocol (web traffic, email, etc.)

UDP
User Datagram Protocol (DNS, DHCP, streaming media)

To start a packet capture:

1. Select the desired **Interface** (LAN or Wireless)
2. Optionally enable **Protocol** filtering by checking the checkbox
3. If protocol filtering is enabled, select the specific protocol type
4. Click the Start button to begin capturing packets

Fig. 8.18 shows the Traffic Diagnostics configuration page.

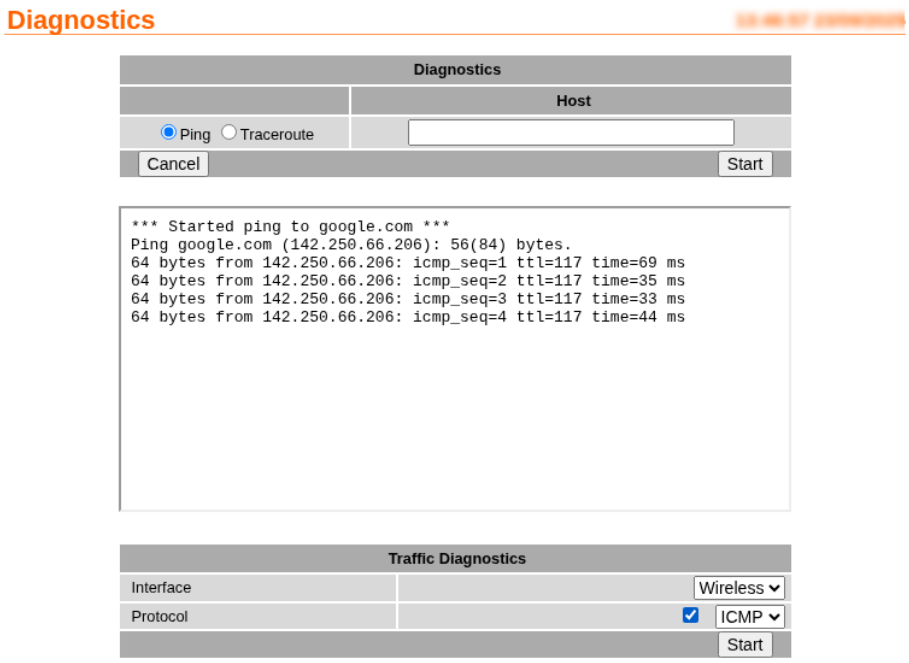


Fig. 8.18: Traffic Diagnostics configuration.

Once the capture begins, the Start button will change to a Stop button, indicating that packet capture is actively running.

To stop the packet capture:

1. Click the Stop button to end the capture session
2. After stopping, a downloadable file link will appear on the page
3. Click the link to download the captured packets as a .pcap0 file

4. The downloaded .pcap0 file can be opened and analyzed using network analysis tools such as Wireshark

Fig. 8.19 shows the Traffic Diagnostics page after a capture has been completed and the download link is available.

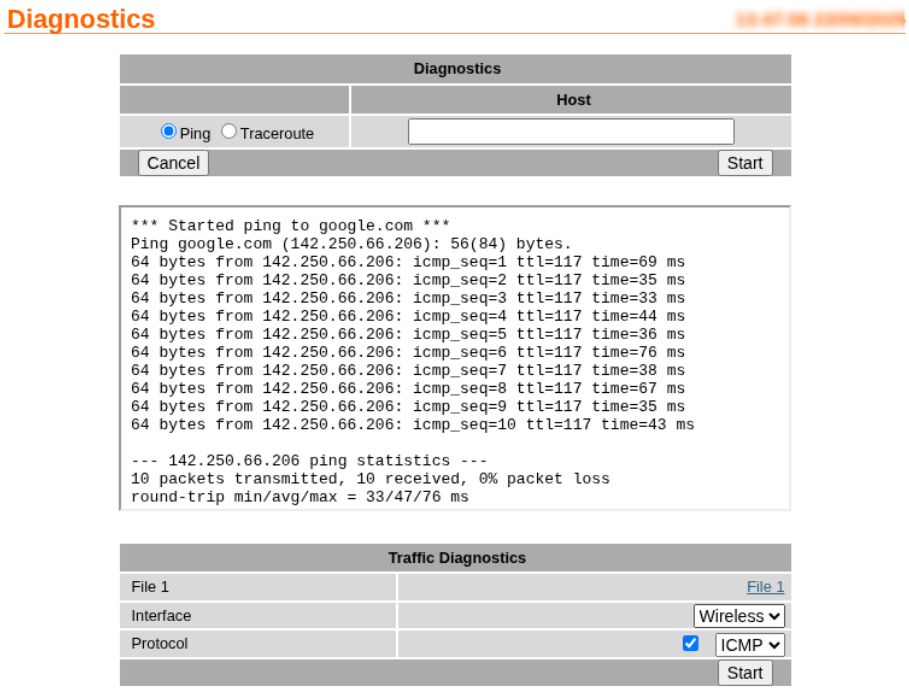


Fig. 8.19: Traffic Diagnostics capture download.

The captured packets are saved in pcap format, which is compatible with network analysis tools such as Wireshark. This allows for detailed examination of network traffic patterns, protocol behaviour, and troubleshooting of connectivity issues.

CHAPTER

NINE

ROUTING

The routing configuration determines how packets arriving from the different interfaces will be delivered to their destination. The routing options are accessed by clicking *Routing* on the main menu, the screen will appear similar to that shown in Fig. 9.1.

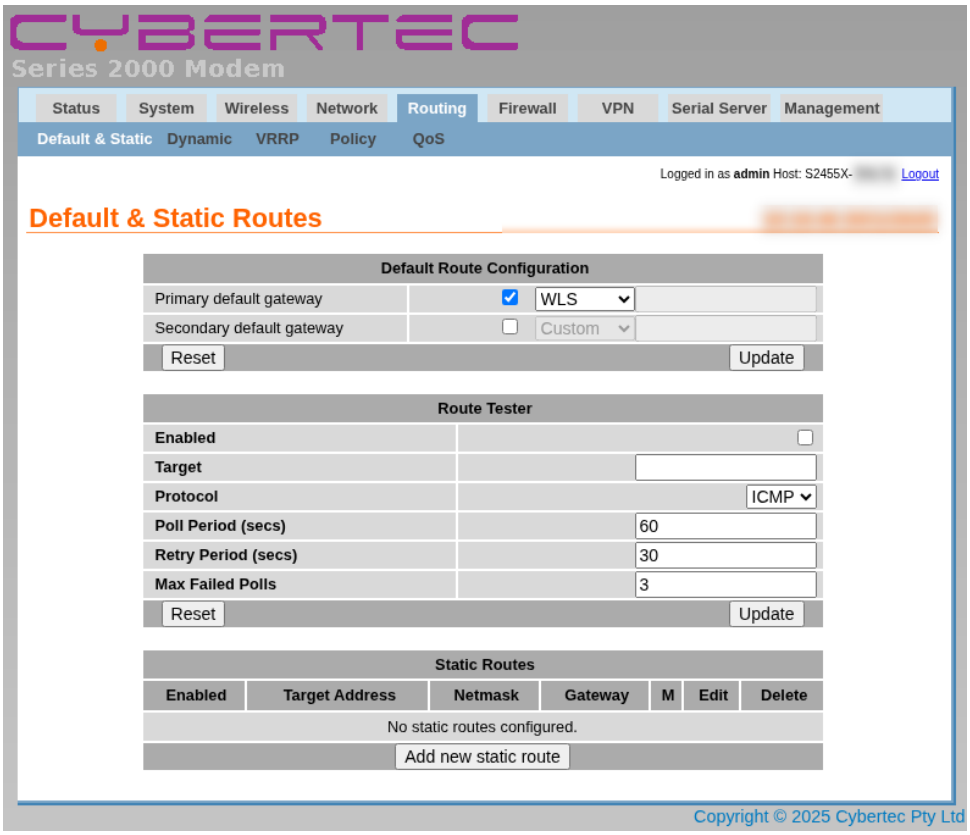


Fig. 9.1: The main routing page.

9.1 Default and Static Routes

The Default & Static Routes are the default routing page and can also be accessed by selecting *Routing* → *Default & Static*. Fig. 9.1 illustrates the Default & Static Routes page with no routes configured.

9.1.1 Default route

The default route is the network route used when no specific route exists for an IP packet's destination address. All the packets for destinations not defined in the routing table are sent to the default route. This route will lead to another router for further routing.

In the default configuration the Primary default gateway is via the wireless interface (**WLS**). In the majority of situations there will be no need to change this setting. A Secondary default gateway can also be configured which will be used in the event of the interface specified as the Primary default gateway being unavailable.

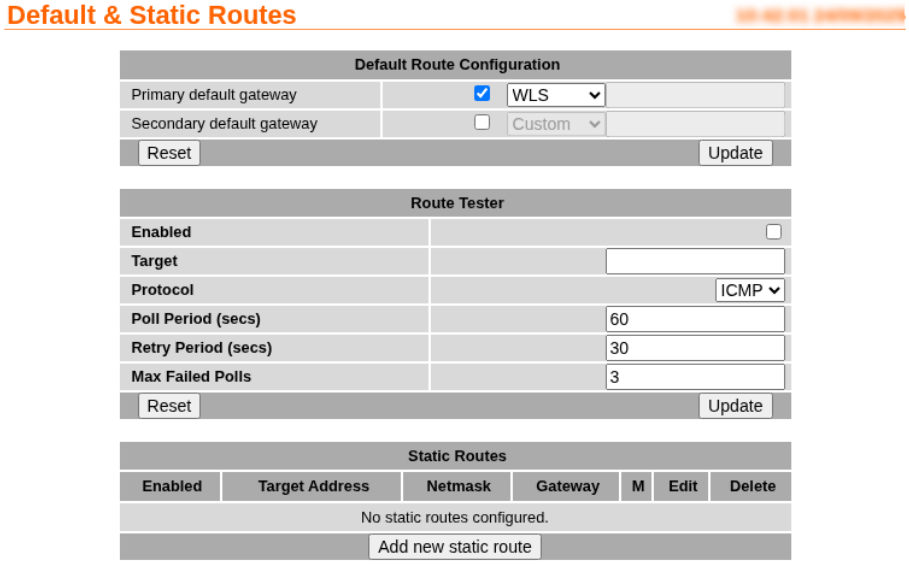


Fig. 9.2: The Default and Static Routes configuration page.

To change the default route select an option from the drop-down list. The possible interfaces include:

WLS
: Wireless interface.

SSL VPN
: The SSL VPN interface. This option is only valid if an SSL VPN has been configured. Refer to Section Virtual Private Network (VPN) for details.

WLS CSD
: The wireless circuit switched data interface. This option is only valid if the unit is operating in Circuit Switched Data (CSD) mode and the PPP server has been enabled.

Serial n
: The serial port, where n is the number of the port. This option is only valid if the serial port is configured to operate in one of the PPP modes.

Custom
: Use the IP address entered in the adjacent field.

Once the required default route has been selected click the Update button to save the change.

To configure a Secondary default gateway check the check-box to enable the Secondary default gateway then select an option from the drop-down list. The possible interfaces are the same as listed above for the Primary default gateway. Once the required default route has been selected click the Update button to save the change.

9.1.2 Route Tester

The **Route Tester** is a diagnostic tool that continuously monitors network connectivity to a specified target. It can be used to verify that routing paths are functioning correctly and to detect network connectivity issues.

The Route Tester can be configured with the following parameters:

Enabled
: Check this checkbox to activate the Route Tester functionality.

Target
Enter the IP address of the target host that you want to monitor. This should be a valid IPv4 address that represents the destination you want to test connectivity to.

Protocol
Select the protocol to use for connectivity testing:

ICMP
Uses ping packets to test connectivity (default)

TCP
Uses TCP connection attempts to test connectivity

Poll Period (secs)
Specifies how often (in seconds) the Route Tester should check connectivity to the target. The default value is 60 seconds.

Retry Period (secs)
Defines the interval (in seconds) between retry attempts when a poll fails. The default value is 30 seconds.

Max Failed Polls
Sets the maximum number of consecutive failed polls before the Route Tester considers the target unreachable. The default value is 3 failed attempts.

To configure the Route Tester:

1. Enable the Route Tester by checking the **Enabled** checkbox
2. Enter the target IP address in the **Target** field
3. Select the appropriate **Protocol** for testing (ICMP or TCP)
4. Configure the timing parameters as needed
5. Click the Update button to save the configuration

The Route Tester will monitor the specified target according to the configured parameters and provide feedback on network connectivity status.

9.1.3 Static routes

Static routes are manually entered routes which direct certain traffic over a network in a fixed or static way. Static routes may be useful for creating exceptions to the default route or for working in complex LAN environments where the configuration is known and consistent.

The diagram in Fig. 9.3 shows a scenario where static routes can be used. In the example, in addition to the 10.10.10.0 subnet the unit is attached to, there is a further subnet (10.10.20.0) reachable via the router at 10.10.10.200. Without a static route, the modem would not know how to handle packets for the 10.10.20.0 subnet and would send them to the default route. With a static route, packets will be correctly forwarded to the router at 10.10.10.200.

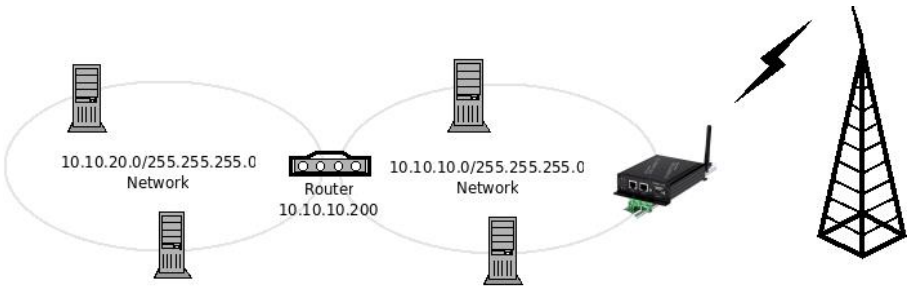


Fig. 9.3: Static routing example

9.1.4 Static route options

The static route options are shown when the Add new static route button is clicked or an existing route is edited. The static route options will be displayed as shown in Fig. 9.4.

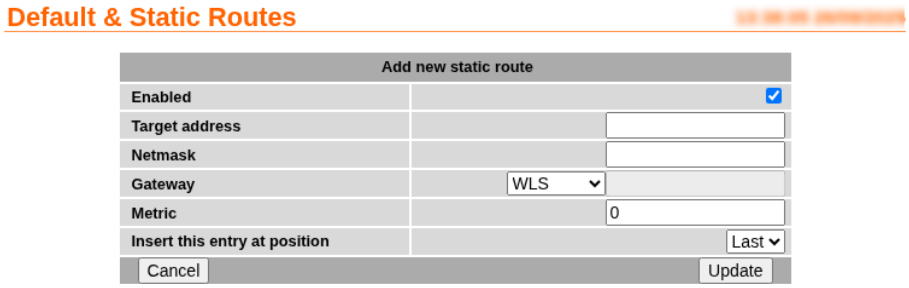


Fig. 9.4: Static route options

The following options can be set for each static route:

Enabled
Set the enabled check box to have the route installed. A route can be temporarily disabled by un-checking this box.

Target address
This is the network or host the static route will target.

Netmask
This is the network mask to apply to the static route. The mask entered should be in IPv4 decimal dotted notation. For a host-only route, the netmask is 255.255.255.255.

Gateway
Determines the gateway that packets whose destination addresses matched the target address will be routed to. The gateway can be one of the following:

WLS
Wireless interface.

SSL VPN
The SSL VPN interface. This option is only valid if an SSL VPN has been configured. Refer to Section Virtual Private Network (VPN) for details.

WLS CSD
The wireless circuit switched data interface. This option is only valid if the unit is operating in Circuit Switched Data (CSD) mode and the PPP server has been enabled.

Serial n
The serial port, where n is the number of the port. This option is only valid if the serial port is configured to operate in one of the PPP modes.

Custom
Use the IP address entered in the adjacent field.

Metric
The metric is used to determine whether one route should be chosen over another, where both routes are possible. The packet will be directed to the route with the lowest metric.

Insert this entry at position
Determines where this entry will be inserted in the list of static routes.

9.1.5 Adding a new static route

From the Default & Static Route page click the Add new static route button, the Add new static route page will be displayed.

An example of adding a new static route is shown in Fig. 9.5. In this example, a new route is to be created that routes all traffic for the 10.10.20.0 subnet via the router at address 10.10.10.200.

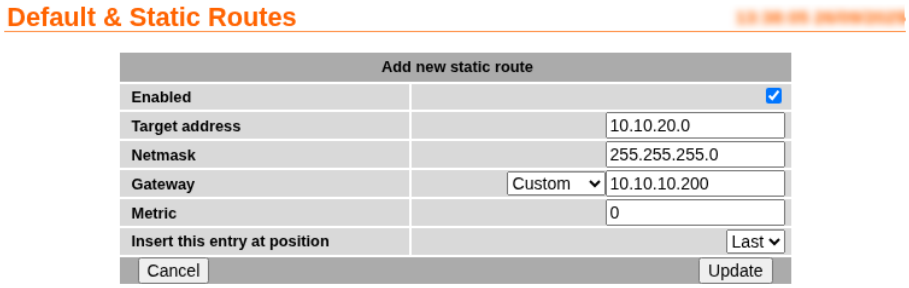


Fig. 9.5: Adding a new static route

To save the new route click the Update button.

The main Default & Static Route page will again be shown with the new route listed, as shown in Fig. 9.6.

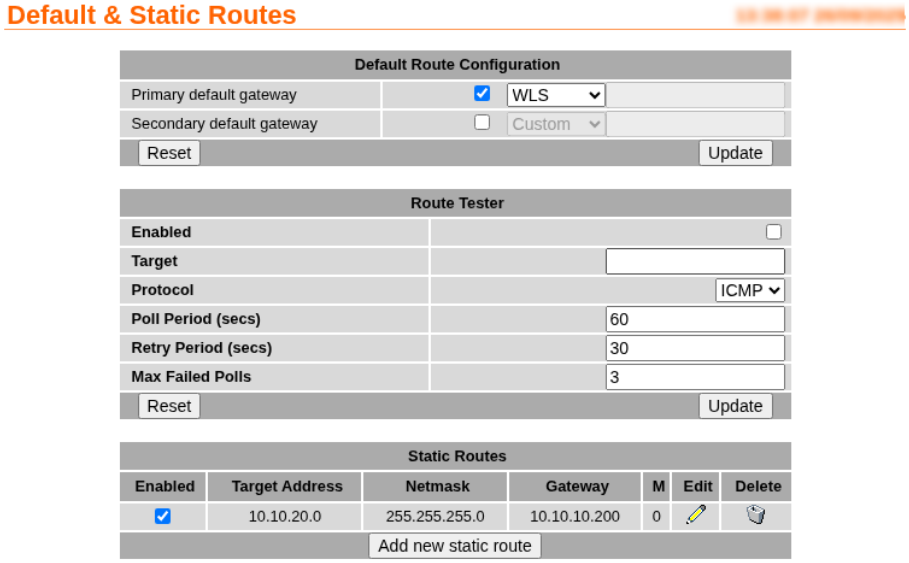


Fig. 9.6: The static route page with a single route

To add a second route, again click the Add new static route button.

In the example shown in Fig. 9.7, a route is created which all route all packets destined for the host 192.168.2.100 via the SSL VPN.

To add the route click the Update button.

The main page will again be shown with the new route added, as seen in Fig. 9.8.

> **Tip**
>
> For the route in this example to work a VPN will need to be configured and established. For details on configuring Virtual Private Networks (VPN) refer to chapter **VPN**.

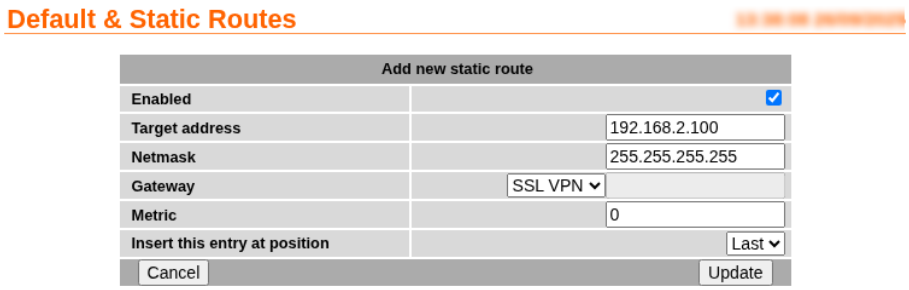


Fig. 9.7: Adding a new static route

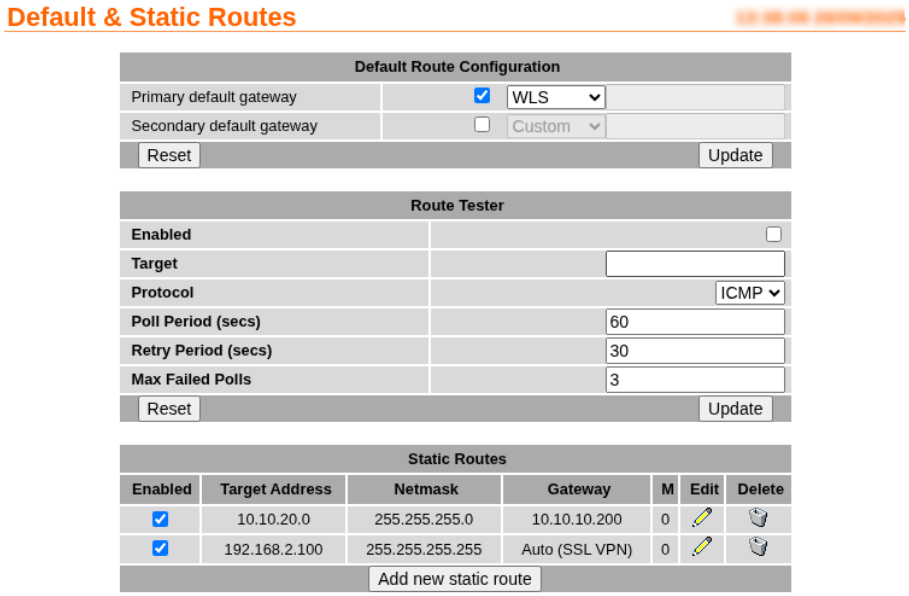


Fig. 9.8: The static route table with two routes

9.1.6 Editing a static route

A static route can be edited by clicking the icon in the **Edit** column of the route to be changed. Once clicked, the details of the route will display in the same table as shown when adding a new route.

As an example, to edit the second route, click the icon in the second row of the table. A page similar to the Add new route page will be displayed, but now showing the details of route 2. Changes to route to the host 192.168.2.200 are shown in Fig. 9.9.

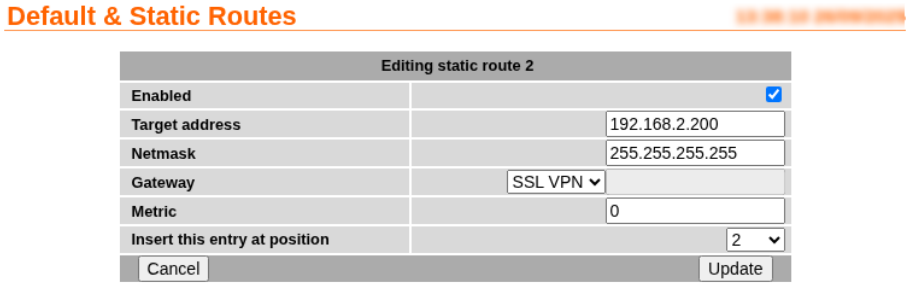


Fig. 9.9: Editing a static route

To save the changes click the Update button or to lose any changes click the Cancel button.

The main page will again be displayed as shown in Fig. 9.10, with the changes for route 2 added to the table.

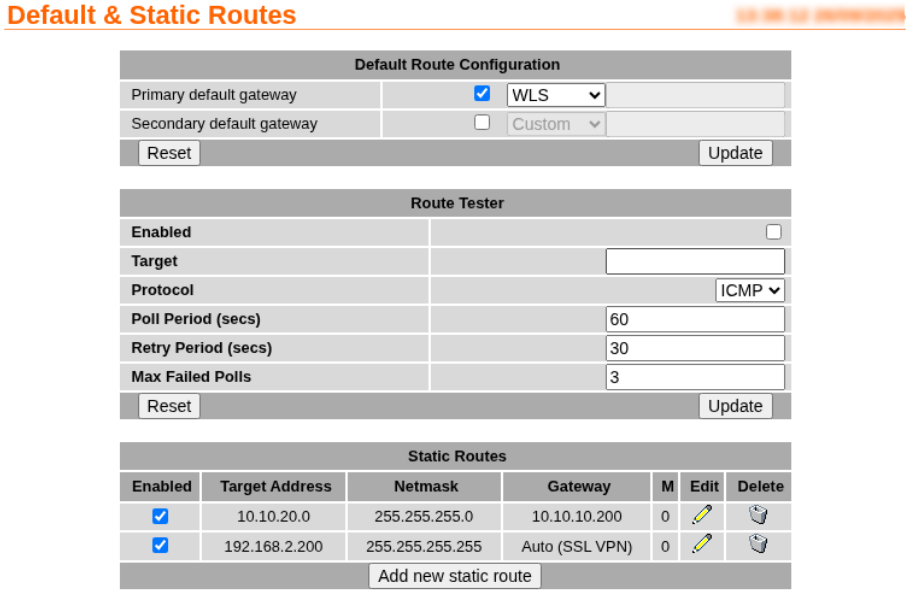


Fig. 9.10: The main route table after editing route two

9.1.7 Deleting a static route

A static route can be deleted by clicking the icon in the **Delete** column of the route to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the route from being deleted.

For example, to delete route two from the table shown in Fig. 9.10, click the icon in row two of the table. A warning box will now be displayed, as shown in Fig. 9.11. Click the OK button to confirm the deletion of the route.

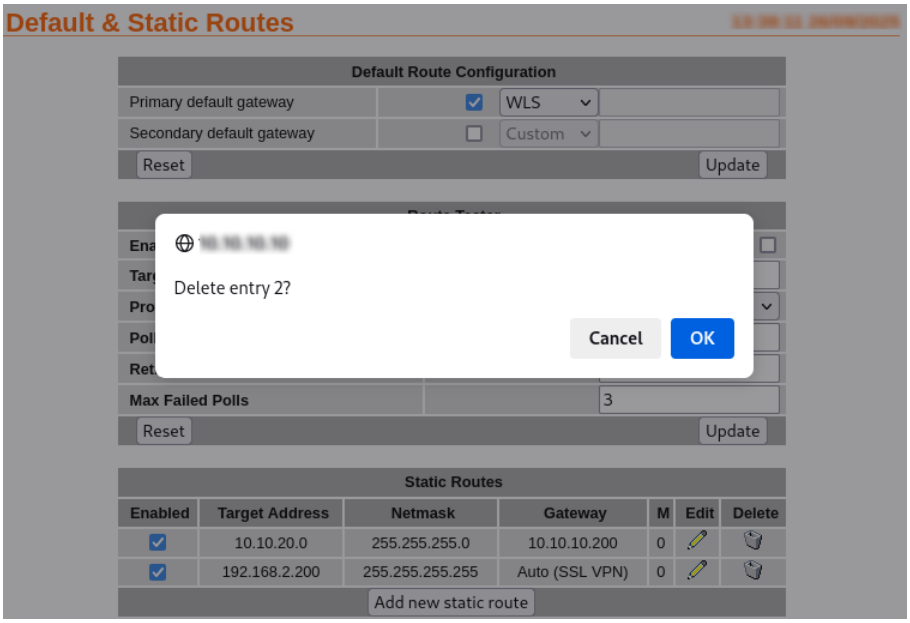


Fig. 9.11: Deleting a static route

The route table will be displayed with the route removed, as shown in Fig. 9.12.

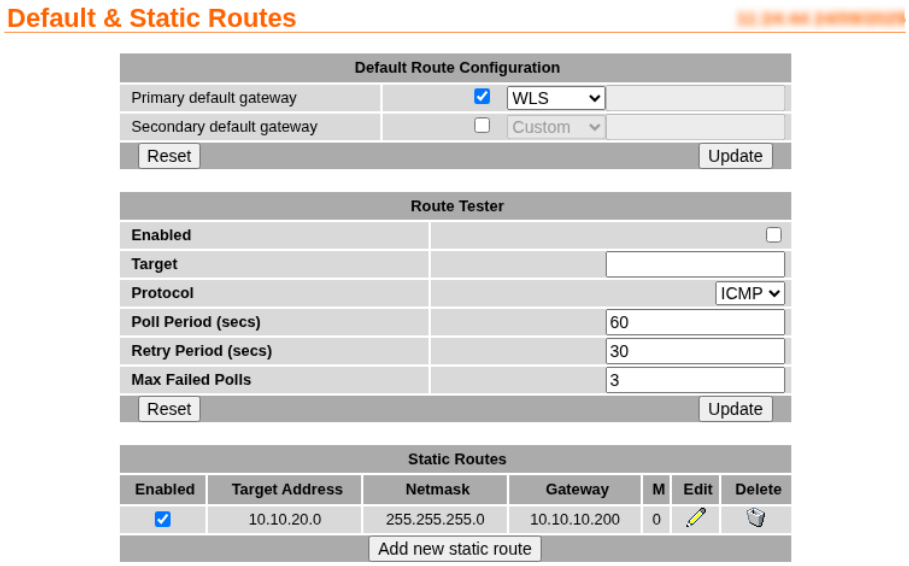


Fig. 9.12: Static route table with route 2 removed

9.2 Dynamic Routing

9.2.1 Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is a protocol for exchanging routing information with neighbouring routers. RIP is a dynamic routing protocol used in local and wide area networks and is supported in many routers. To access the dynamic routing page, select *Routing* → *Dynamic* a page similar to that shown in Fig. 9.13 will be displayed.

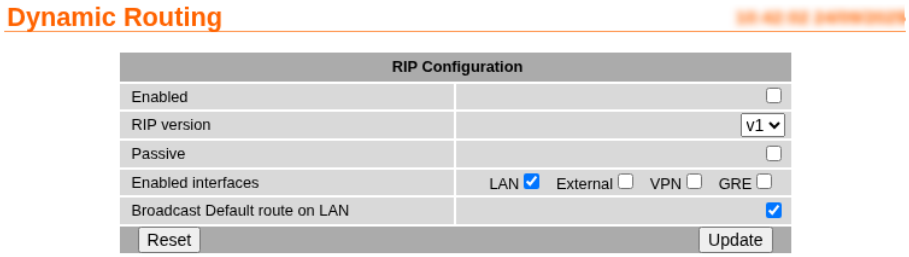


Fig. 9.13: Dynamic routing

9.2.2 Enabling RIP

The RIP function is enabled in the **RIP Configuration** table. The description below explains the fields:

Enabled
When set, the dynamic routing function will be enabled.

RIP Version
This field determines the protocol version of RIP to be used. Select the version to match that used by neighbouring routers.

Passive
When set, packets received on the LAN interface will not be actively broadcast.

Enabled interfaces
Select the interfaces for which RIP will be enabled. More than one interface may be selected.

Broadcast Default route on LAN
When set, the default route will be broadcast on the LAN interface.

Click the Update button to save and commit the changes.

9.3 Virtual Router Redundancy Protocol (VRRP)

9.3.1 Description

The Virtual Router Redundancy Protocol (VRRP) is designed to increase the availability of the default gateway servicing hosts on a subnet. VRRP is a standardised protocol defined in RFC 3768. Vendors such as Cisco include implementations in their router products.

VRRP achieves redundancy by creating a "virtual gateway". At any time, only one of the VRRP-enabled routers functions as the virtual gateway. The virtual gateway address is configured into hosts on the local network as their default gateway. VRRP routers take part in elections to decide who will become the master router. The master router then assumes the IP address of the virtual gateway and becomes the path for network traffic.

Fig. 9.14 shows a two modem set-up using VRRP. Router A and Router B communicate via multicast messages to determine who will be the master router. As Router A has higher priority it will become the master in preference to Router B. Should Router B detect that Router A is no longer functioning, it will assume the role of the master router. Once Router A returns, it becomes the master again.

The time for Router B to detect that Router A has failed is determined by the advertising interval. The advertising interval determines how frequently the master router notifies other routers of its state. If Router B is not notified of the status of Router A for more than 3 times the advertising interval, Router B will assume the failure of Router A and become the master. The advertising interval can be set to a low value (as short as 1 second), however, the lower the value, the greater the volume of broadcast traffic on the local network.

To access the VRRP configuration, select *Routing* → *VRRP* a page similar to that shown in Fig. 9.15 will be displayed.

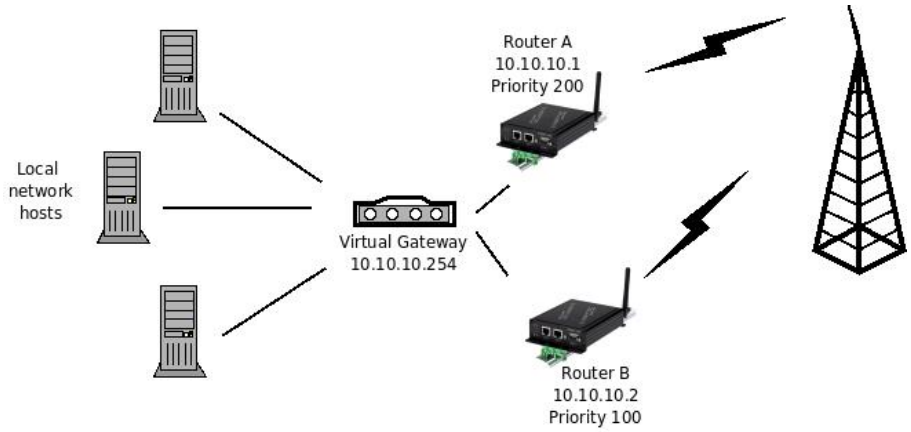


Fig. 9.14: VRRP network scenario

Virtual Router Redundancy Protocol

VRRP Configuration		
Enabled		☐
Virtual router ID		1
Virtual router IP address		0.0.0.0
Priority		100
Advertising interval (secs)		1
Enable Extended Logging		☐
Conditions		
Interface	Advertise when up	None
	Stable Time (sec)	10
Keepalives	Enable	Disabled
Reset		Update

Fig. 9.15: VRRP configuration

9.3.2 VRRP Configuration

The following fields need to be configured to enable VRRP:

VRRP Configuration Enabled
When set, the VRRP function will be enabled.

Virtual router ID
The virtual router ID (VRID) is common to all physical routers that are part of the same virtual router group. Set this field to match the ID used by the virtual group.

Virtual router IP address
This is the IP address of the virtual gateway. It is common to all physical routers in the same virtual router group.

Priority
This field determines how highly this router will rank in elections for a new master. A router with a higher priority will be chosen in preference to a router with lower priority. The valid range of priorities is 1 to 254.

Advertising interval (secs)
This field determines the frequency with which the router will multicast its status to other router while it is the master. The value entered is in seconds.

Enable Extended Logging
Check to enable verbose logging. Normally only used for debugging and system set up.

Conditions Interface-Advertise when up
When an interface is selected the VRRP function will be disabled until the interface is connected and available. This prevents the unit from becoming the master router when no onward connection is available.

Keepalives-Enable
Keep-alives are used to ensure the gateway service is available. Keep-alives can be enabled by selecting Poll at fixed interval. When selected (refer to Fig. 9.16) the following configuration options will appear:

Poll Period (secs)
The polling period in seconds.

Retry Period (secs)
Check box to enable re-tries if initial poll fails, the text box is for the re-try time in seconds.

Maximum failed polls
The maximum number of failed polls.

Estimated detection (secs)
The estimated minimum and maximum time for a failure to the detected.

Poll
The poll type either ICMP (Ping) or TCP Socket and the remote address to poll.

Click the Update button to save and commit the changes.

> **Tip**
>
> Once enabled, VRRP will change the MAC address of the LAN interface. This may make the internal web server temporarily unavailable until the change in address has propagated.

9.3.3 VRRP Configuration Example

This example will describe the VRRP configuration for the two modems described in the network diagram of Fig. 9.14 on the previous page. As the two devices are in the virtual router group the majority of the settings are the same. The exception is the priority which must be higher for Router A as it is to be the master. The settings for each device is listed below and shown in Fig. 9.17 for Router A and Fig. 9.18 for router B.

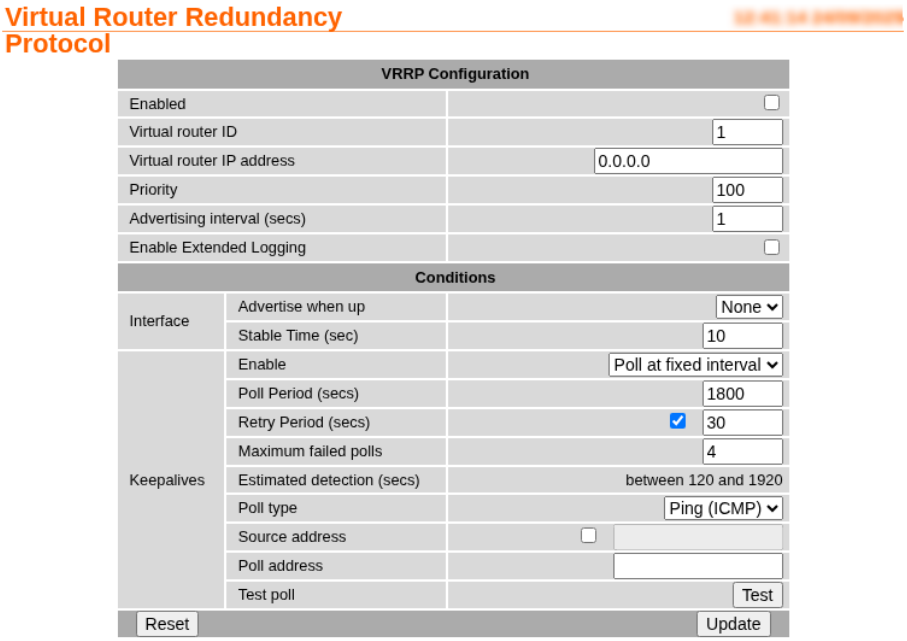


Fig. 9.16: VRRP configuration with polling options shown.

VRRP Configuration Enabled
Checked to enable.

Virtual router ID
Set to 1 (the default).

Virtual router IP address
Set to the IP address 10.10.10.254

Priority
Router A set to 200 and Router B set to 100 (the default).

Advertising interval
Set to 1 second (the default).

Enable Extended Logging
Disabled (not checked) for both devices.

Conditions Interface-Advertise when up
Set to the wireless interface WLS

Keepalives-Enable
Poll at fixed interval

Poll Period (secs)
1800

Retry Period (secs)
Check to enable re-tries and set the retry time for 30 seconds

Maximum failed polls
Set maximum number of poll failures to 4

Estimated detection (secs)
Calculated

Poll
Set poll type either Ping (ICMP) and the remote address to poll as 192.168.0.2.

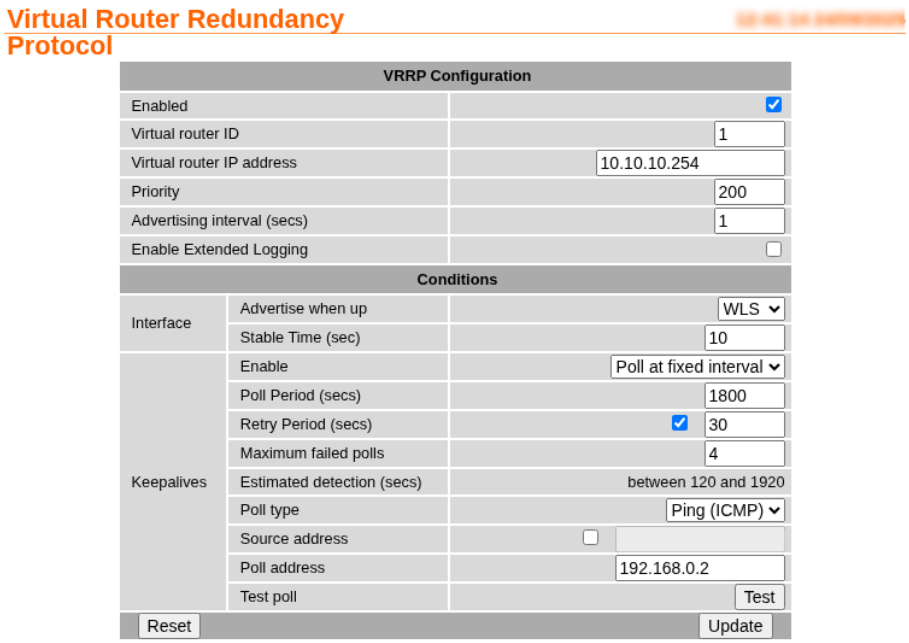


Fig. 9.17: VRRP configuration for Router A

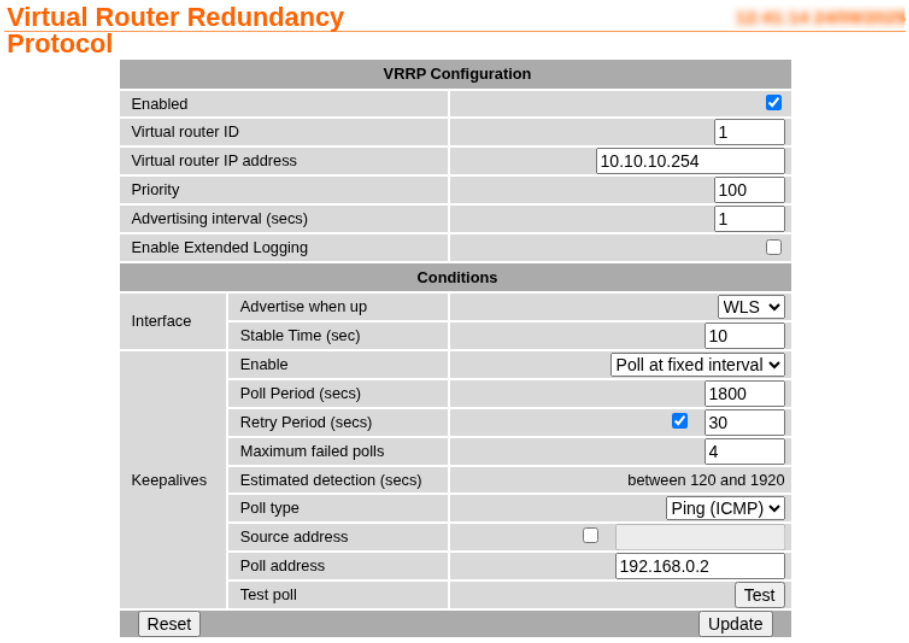


Fig. 9.18: VRRP configuration for Router B.

9.4 Policy Routing

9.4.1 Description

Policy routing is an advanced routing feature that allows packets to be routed based on which of the modem's network interfaces they arrive on, the protocol type or the source or destination address. Conceptually a policy route is similar to a static route, but, as a policy route can match on more attributes than a packet's destination address, they allow for greater flexibility.

To access the policy route configuration, select *Routing* → *Policy* a page similar to that shown in Fig. 9.19 will be displayed.

Fig. 9.19: Policy routes

9.4.2 Policy route options

The policy route options are shown when the **Add new policy route** button is pressed or an existing route is edited. The policy route options will be displayed as shown in Fig. 9.20.

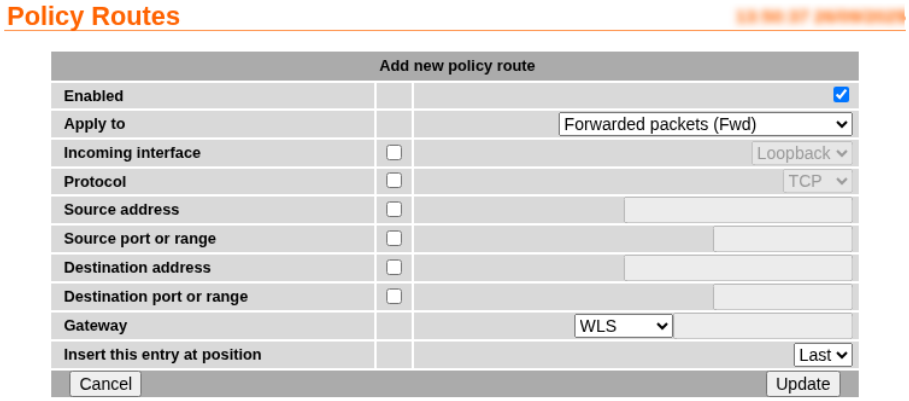


Fig. 9.20: Policy route options

The following options can be set for each policy route:

Enabled
: Set the enabled check box to have the route installed. A route can be temporarily disabled by un-checking this box.

Apply to
: Policy routes can be applied at two separate points in the modem:

  Forwarded packets
  : The route will be applied to packets that are received from one network interface and then routed out another network interface.

  Locally generated packets
  : The route will be applied to packets generated by one of the modem's internal services.

Incoming interface
: If selected, packets will be matched based on the network interface they have been received on. Note that this can't be applied to **Locally generated packets** as they have been generated by the modem itself.

Protocol
If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address
If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the filter applied to them.

Source port or range
If selected, packets will be matched based on their TCP or UDP source port. Either an individual port (for example, 443) or a range of ports (80-143) can be entered.

Destination address
Similar to the **Source address**, but instead matching on the destination address.

Destination port or range
Similar to the **Source port or range,** but instead matching on the destination port.

Gateway
Determines the gateway that packets that meet all of the matching criteria for the route will be routed to. The gateway can be one of the following:

WLS
Wireless interface.

SSL VPN
The SSL VPN interface. This option is only valid if an SSL VPN has been configured. Refer to Section Virtual Private Network (VPN) for details.

WLS CSD
The wireless circuit switched data interface. This option is only valid if the unit is operating in Circuit Switched Data (CSD) mode and the PPP server has been enabled.

Serial n
The serial port, where n is the number of the port. This option is only valid if the serial port is configured to operate in one of the PPP modes.

Custom
Use the IP address entered in the adjacent field.

Insert this entry at position
Determines where this entry will be inserted in the list of policy routes.

9.4.3 Adding a new policy route

From the main Policy Route page click the Add new policy route button. This will select the Add new policy route page. An example of adding a new policy route is shown in Fig. 9.21. In this example, a new route is to be created that routes all outgoing mail traffic (SMTP, TCP port 25) received from the LAN interface via the gateway at address 10.10.10.1.

It can be seen in the example that in the centre column, **Incoming interface, Protocol** and **Destination port or range** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

To save the new route click the Update button. The main Policy Route page will again be shown with the new route listed, as shown in Fig. 9.22.

To add a second route, again click the Add new policy route button. In the example shown in Fig. 9.23, a policy route is created which will route all packets received from the LAN interface, from IP address 10.10.10.50 via the SSL VPN. Again notice that in the centre column, **Incoming interface** and **Source address** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

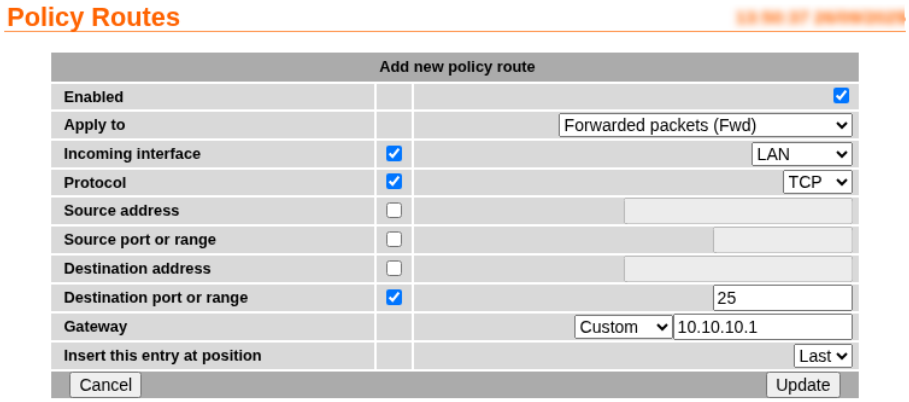


Fig. 9.21: Adding a new policy route

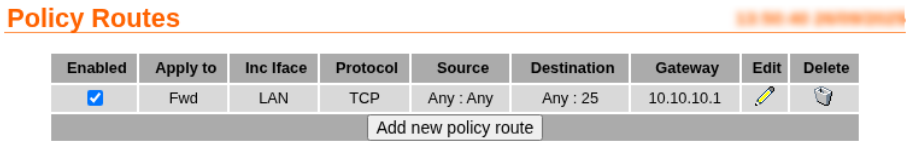


Fig. 9.22: The policy route page with a single route

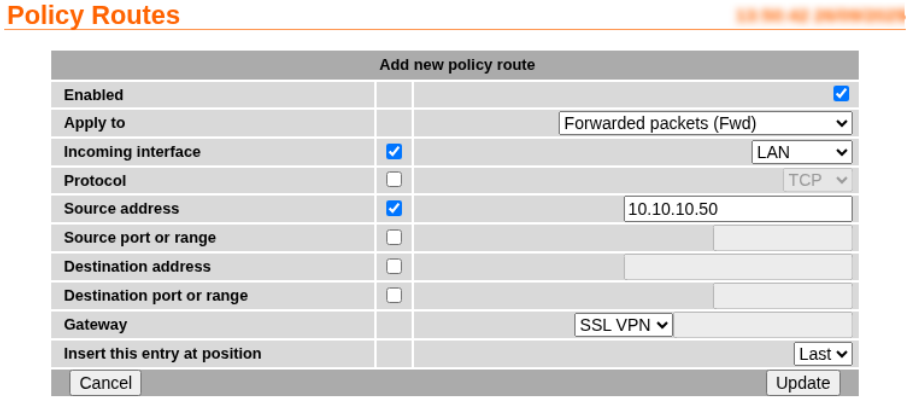


Fig. 9.23: Adding a second policy route

To add the route click the Update button. The main page will again be shown with the new route added, as seen in Fig. 9.24.

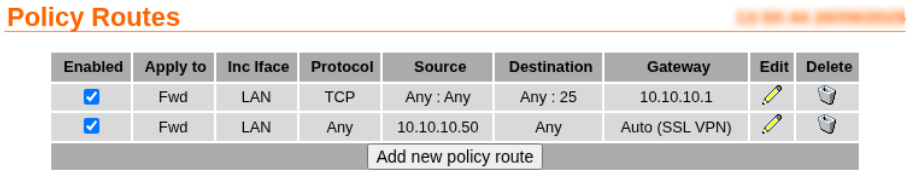


Fig. 9.24: The policy route table with two routes

9.4.4 Editing a policy route

A policy route can be edited by clicking the icon in the **Edit** column of the route to be changed. Once clicked, the details of the route will display in the same table as shown when adding a new route.

As an example, to edit the second route, click the icon in the second row of the table. Changes that add destination address matching to the criteria are shown in Fig. 9.25.

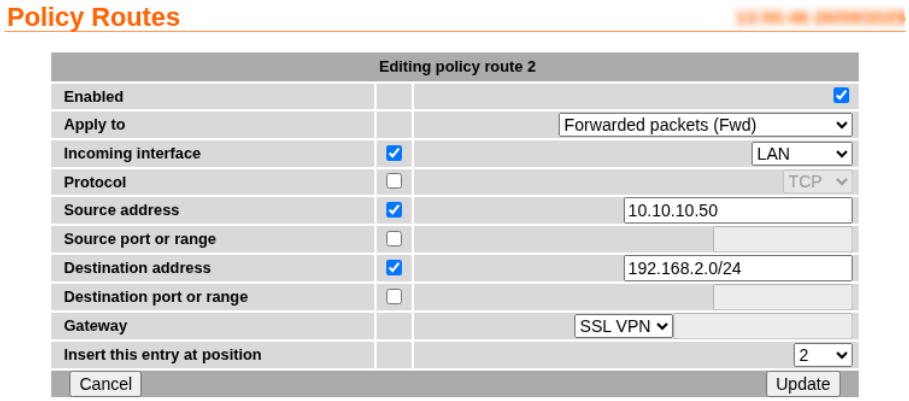


Fig. 9.25: Editing a policy route

To save the changes click the Update button or to lose any changes click the Cancel button. The main page will again be displayed as shown in Fig. 9.26, with the changes for route 2 added to the table.

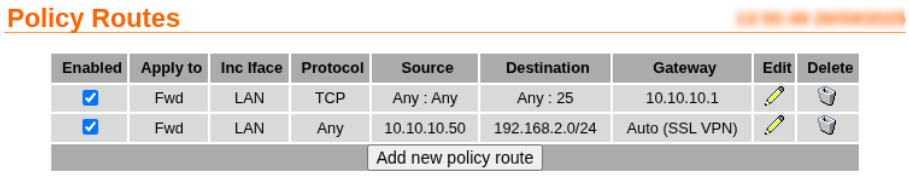


Fig. 9.26: The main route table after editing route two

9.4.5 Deleting a policy route

A policy route can be deleted by clicking the icon in the **Delete** column of the route to be deleted. A warning box willbe displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the route from being deleted.

For example, to delete route two from the table shown in Fig. 9.26, click the icon in row two of the table. A warning box will now be displayed, as shown if Fig. 9.27. Click the OK button.

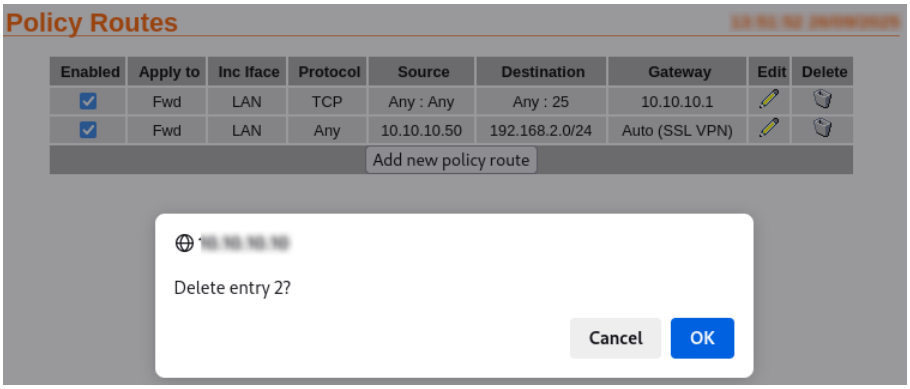


Fig. 9.27: Deleting a policy route

The route table will be displayed with the route removed, as shown in Fig. 9.28.

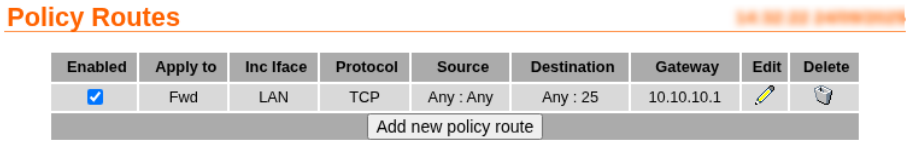


Fig. 9.28: Policy route table with route two removed

9.5 Quality of Service Routing

9.5.1 Description

For bandwidth intensive applications, such as live video or Voice-over-IP (VOIP), it may be desirable to have certain types of traffic prioritised for transmission out the Wireless interface in preference to other traffic. For example, live video packets are more time critical than outgoing email and should be prioritised as such.

The QoS implementation works by dividing the outgoing queue to selected interface into three queue levels:

- High (minimum 60% of bandwidth)
- Standard (minimum 30% of bandwidth)
- Low (minimum 10% of bandwidth)

Where a queue is not using all of its available bandwidth, queues below will expand their bandwidth to ensure full link utilisation. For example, if there is currently no high priority traffic queued, standard traffic will be able to use up to 90% of the available bandwidth.

Configuring the QoS function is performed in two steps:

- Setting the basic options (enabling QoS and setting the available bandwidth)
- Configuring multiple rules to classify packets into the three different priority queues.

To access the QoS configuration, select *Routing* → *QoS* a page similar to that shown in Fig. 9.29 will be displayed.

9.5.2 Basic QoS options

To enable the QoS feature, the following fields must be set:

QoS enabled
: When set, QoS is activated for the indicated interface.

Max uplink rate
: Set this to the maximum bit rate attainable for the indicated interface. It is important that this value be correct, as it will be used to determine the bandwidth allocations for each priority level.

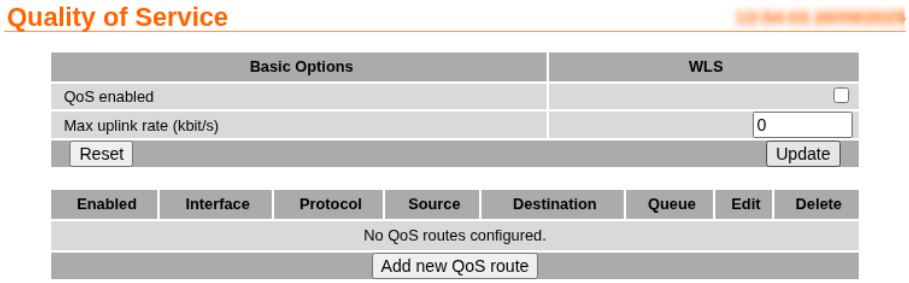


Fig. 9.29: Quality of Service

Tip

It may be necessary to test the interface to determine the maximum bandwidth. This value could vary between installations.

Click the Update button to save and commit the changes.

9.5.3 Basic QoS Configuration

As an example of how to complete the basic QoS configuration, assume the maximum uplink bandwidth is 350kbits/sec. QoS would then be set with the following values:

QoS enabled
: check to enable QoS

Max uplink rate
: Set to 350.

Fig. 9.30 illustrates the settings for this example.

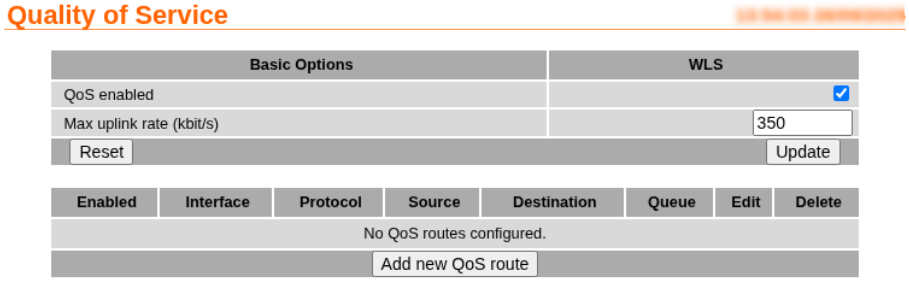


Fig. 9.30: Quality of Service configuration with the uplink rate set.

9.5.4 QoS route options

The QoS route options are shown when the Add new QoS route button is clicked or an existing route is edited by clicking the  icon in the **Edit** column of the route to be changed . The QoS route options will be displayed as shown in Fig. 9.31.

The following options can be set for each QoS route:

Enabled
: Set the enabled check box to have the route installed. A route can be temporarily disabled by un-checking this box.

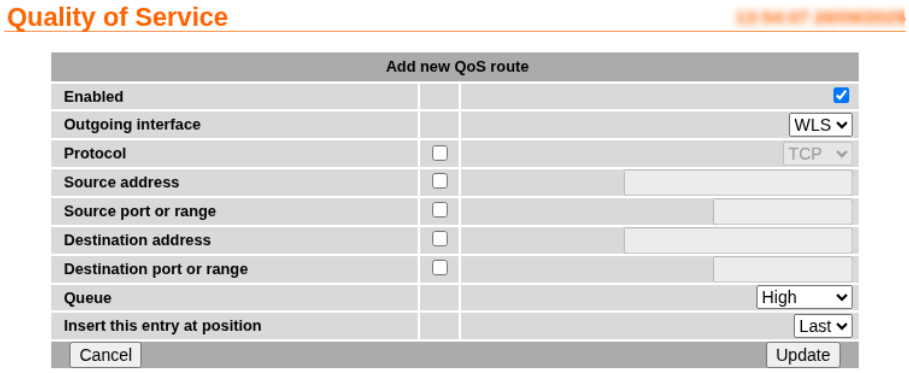


Fig. 9.31: QoS route options

Protocol
: If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address
: If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the route applied to them.

Source port or range
: If selected, packets will be matched based on their TCP or UDP source port. Either an individual port (for example, 443) or a range of ports (80-143) can be entered.

Destination address
: Similar to the **Source address**, but instead matching on the destination address.

Destination port or range
: Similar to the **Source port or range,** but instead matching on the destination port.

Queue
: Sets the priority queue that packets who meet all of the matching criteria for the route will be assigned to.

Insert this entry at position
: Determines where this entry will be inserted in the list of QoS routes.

9.5.5 Adding a new QoS route

From the main QoS Route page click the Add new QoS route button. This will select the Add new QoS route page. An example of adding a new QoS route is shown in Fig. 9.32. In this example, a new route is to be created that classifies all traffic from the host 10.10.10.95 with TCP source port 80 to the high priority queue.

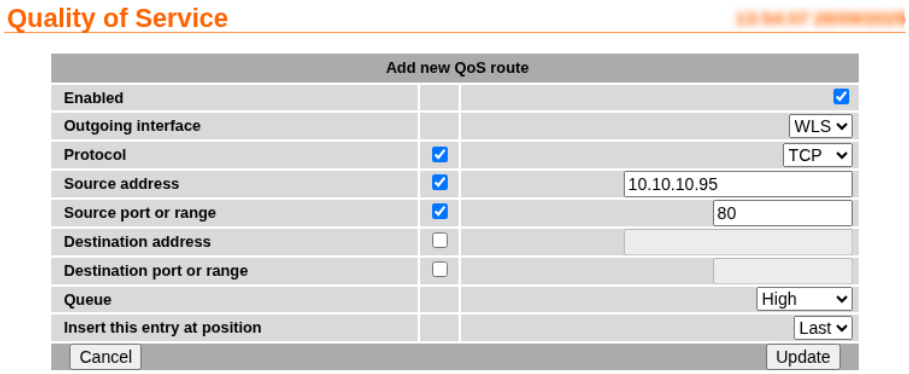


Fig. 9.32: Adding a new QoS route

It can be seen in the example that in the centre column **Protocol** and **Source address** and **Source port or range** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

To save the new route click the Update button. The main QoS Route page will again be shown with the new route listed, as shown in Fig. 9.33.

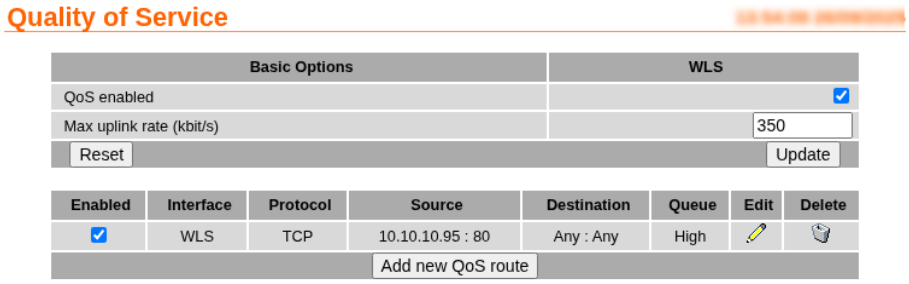


Fig. 9.33: The QoS route page with a single route

To add a second QoS route, again click the Add new QoS route button. In the example shown in Fig. 9.34, a QoS route is created which will classify all packets destined for an SMTP email server (TCP port 25) to the low priority queue. Again notice that in the centre column, **Protocol**, **Destination address** and **Destination port or range** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

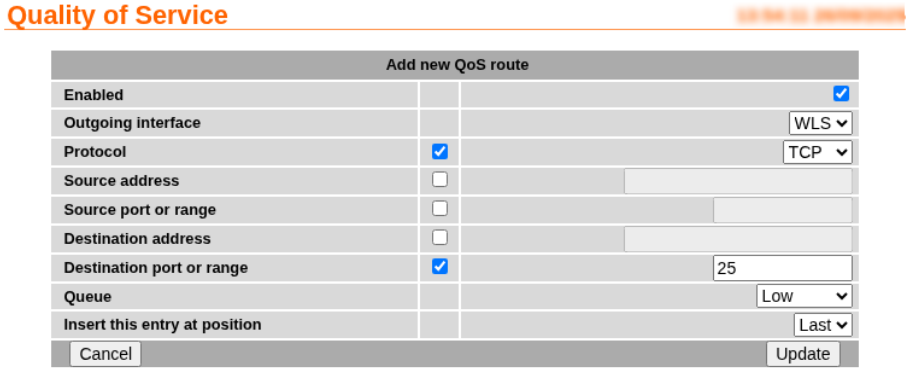


Fig. 9.34: Adding a new QoS route

To add the route click the Update button. The main page will again be shown with the new route added, as seen in Fig. 9.35.

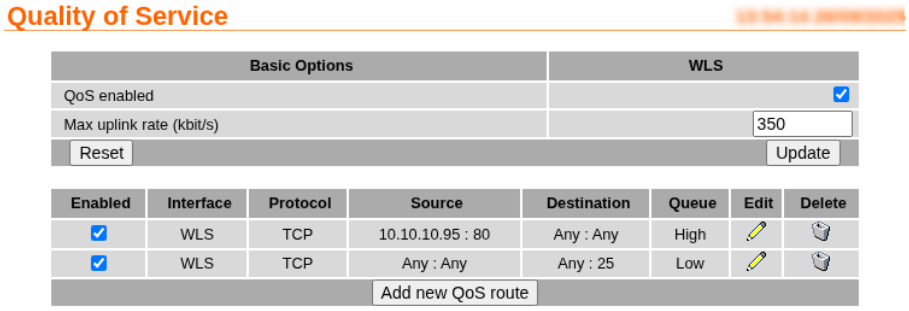


Fig. 9.35: The QoS route table with two routes

9.5.6 Editing a QoS route

A QoS route can be edited by clicking the icon in the **Edit** column of the route to be changed. Once clicked, the details of the route will display in the same table as shown when adding a new route.

As an example, to edit the second route, click the icon in the second row of the table. A page similar to the Add new route page will be displayed, but now showing the details of route 2. Changes that add destination address matching to the criteria are shown in Fig. 9.36.

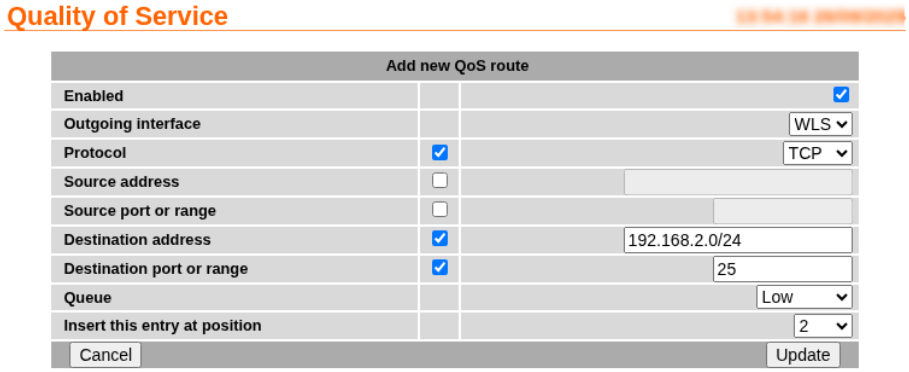


Fig. 9.36: Editing a QoS route

To save the changes click the Update button or to lose any changes click the Cancel button. The main page will again be displayed as shown in Fig. 9.37, with the changes for route 2 added to the table.

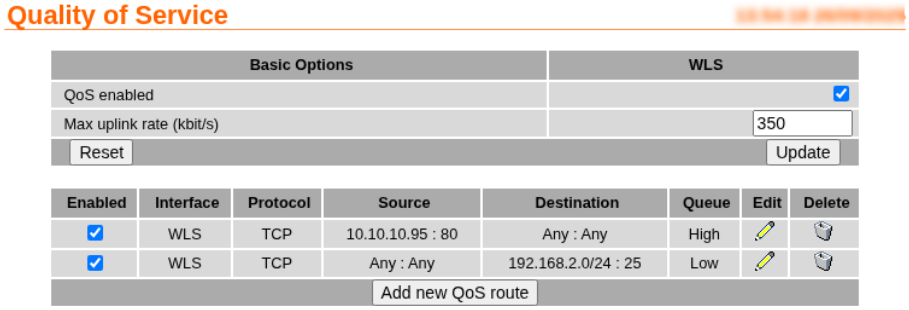


Fig. 9.37: The main route table after editing route two

9.5.7 Deleting a QoS route

A QoS route can be deleted by clicking the icon in the **Delete** column of the route to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the route from being deleted.

For example, to delete route two from the table shown in Fig. 9.37, click the OK icon in row two of the table. A warning box will now be displayed, as shown if Fig. 9.38. Click the OK button to confirm.

The route table will be displayed with the route removed, as shown in Fig. 9.39.

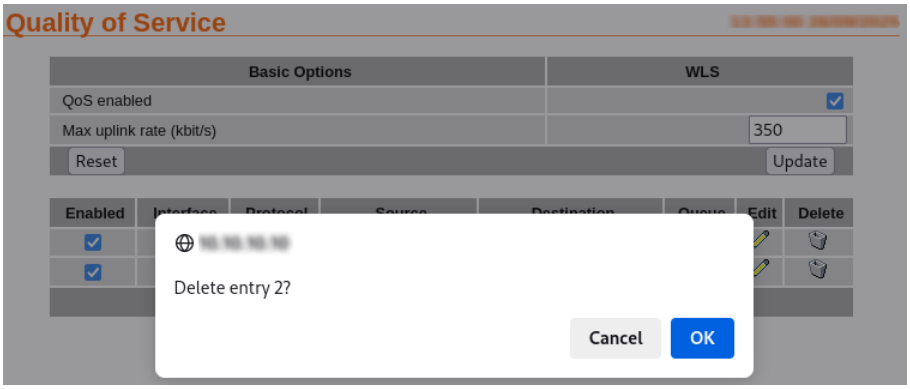


Fig. 9.38: Deleting a QoS route

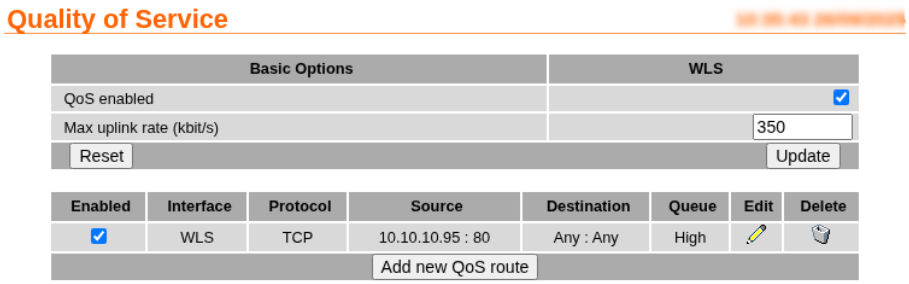


Fig. 9.39: QoS route table with route two removed

CHAPTER

TEN

FIREWALL

The Stateful Packet Inspection (SPI) Firewall controls the connections from the wireless port to the LAN ports and to the modem itself. The firewall can be used to limit the connections that can be established to or via the router. For example, if the router is only to be used for serial communications then the firewall can be set-up to only allow connections through to the serial server (which connects to the serial ports).

The firewall configuration is accessed by selecting the **Firewall** tab from the main menu. When selected the page shown in Fig. 10.1 will be displayed.

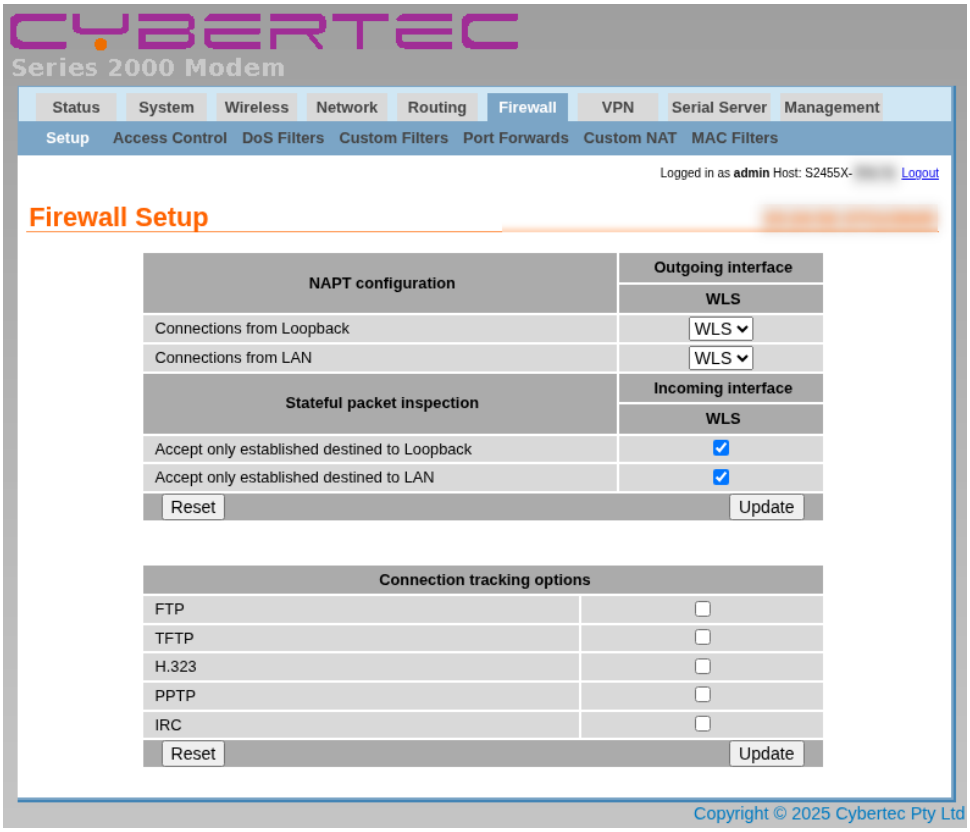


Fig. 10.1: Main Firewall page

10.1 Firewall Setup

The firewall configuration is accessed by selecting the *Firewall* → *Setup* from the menu. When selected the page will provide the basic configuration details for the firewall as shown in Fig. 10.2.

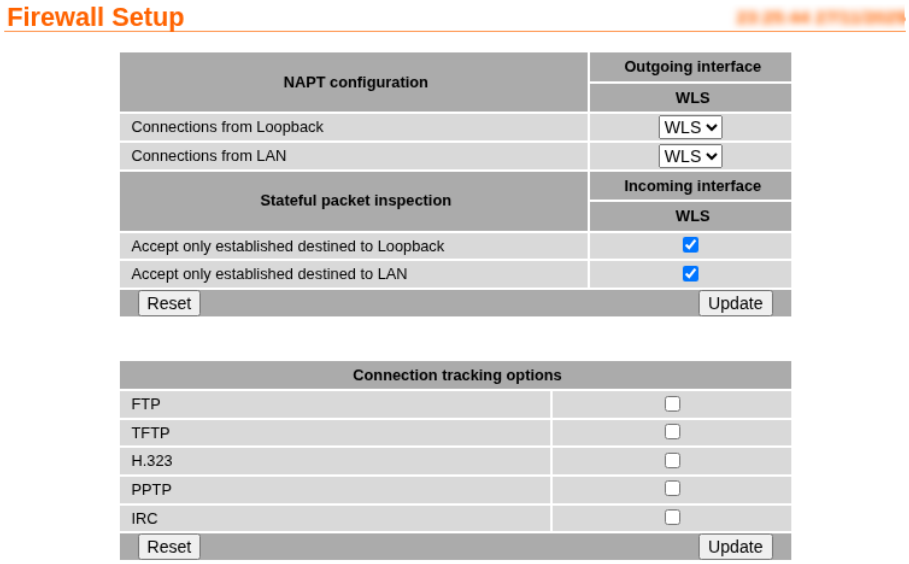


Fig. 10.2: Basic firewall configuration

10.1.1 Network Address and Port Translation (NAPT)

As connection pass from the LAN or Loopback interface and out the WAN (wireless or ADSL) port, the firewall can perform Network Address and Port Translation (NAPT). When set, this option will cause the firewall to substitute the address of the WAN port for the source address of connections received from the LAN or Loopback interface. This is most useful where the LAN or Loopback is a private network and the WAN port has a public address.

In some cases, for example, if connected to an IP WAN that supports direct routing to the LAN network, it may be desirable to disable the NAPT function. This will allow clients on the LAN to be directly addressed without the need for port forwards.

To disable NAPT, un-check the **Connections from LAN** and/or **Connections from Loopback** check-boxes and click the Update button to save and commit the changes.

10.1.2 Stateful Packet Inspection (SPI)

The firewall can function in Stateful Packet Inspection (SPI) mode. When enabled, the firewall will track the state of each connection passing through it (for example, TCP streams) and only allow packets belonging to a known connection to enter from the WAN port. In most cases, SPI should be enabled for greater security. When disabled, the firewall will allow all incoming packets from the WAN port to be forwarded through.

In some cases, for example, if connected to an IP WAN that supports direct routing to the LAN network, it may be desirable to disable the SPI function. This will allow clients on the LAN to be directly addressed without the need for port forwards.

To disable Stateful Packet Inspection (SPI), un-check the **Accept only established destined to LAN** and/or **Accept only established destined to Loopback** check-boxes and click the Update button to save and commit the changes.

10.1.3 Connection tracking options

The firewall can be configured to provide connection tracking and NAT support for a number of additional protocols. The protocols are listed in Table 10.1. To enable support for a protocol, click the check-box for the protocol and click the Update button to save and commit the changes.

Table 10.1: Firewall Connection tracking options

Protocol	Description
FTP	Adds support for active mode File Transfer Protocol
TFTP	Adds support for the Trivial File Transfer Protocol
H.323	Adds support for the H.323 voice and video-conferencing protocol
PPTP	Adds support for the Point-to-point Tunnelling Protocol
IRC	Adds support for the Internet Relay Chat protocol

10.2 Access Control

10.2.1 Description

The Access Control page allows configuration of the firewall to allow or deny access to internal services of the modem from the wireless port and VPN tunnels. By default, the firewall will block access from the wireless port to all internal services such as the web server, and allow access to all internal services from the VPN tunnels. In certain situations it may be desired to enable access to some services from the wireless port or to disable access to some services from the VPN tunnels, by changing the settings on this page.

The port numbers for internal services are the standard port numbers for the service type, for example, port 80 is used for the web server. It is possible to change the port number for a particular service. This may be a requirement if a conflict exists with a particular port or service.

To access the Access Controls, select the *Firewall → Access Control* from the menu. When selected the page will show the access control details for the firewall as shown in Fig. 10.3.

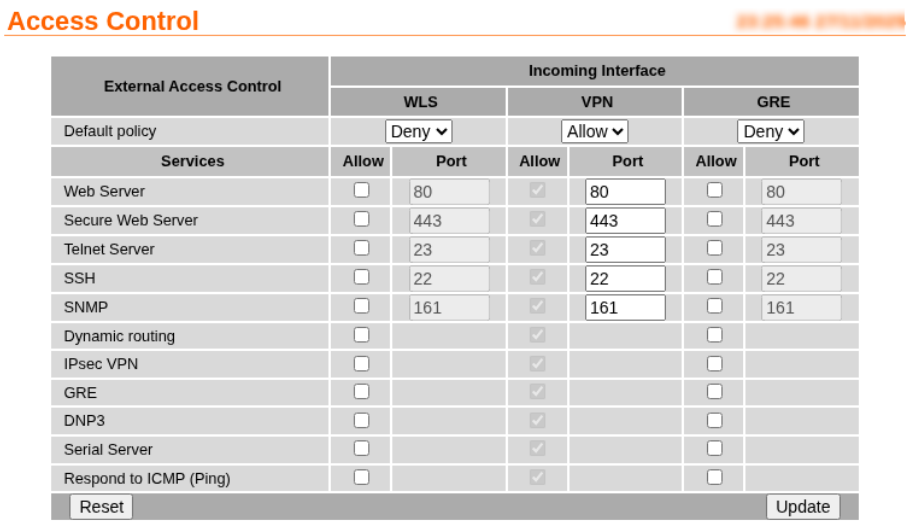


Fig. 10.3: Firewall access control options

10.2.2 Accessing modem services from the WAN port or VPN tunnels

The External Access table provides controls for which services can be accessed from the WAN (Wireless and ADSL) interface and VPN tunnels. By default, the modem will block all requests received on the WAN interface and allow all requests received from VPN tunnels.

There are several modes for determining which services can be accessed:

No access
: All incoming requests are dropped. Set the **Default policy** set to **Deny** and check no boxes in the **Allow** column.

Restricted access
Incoming requests for particular services will be allowed. Set the **Default policy** to **Deny** and check the boxes for the desired services in the **Allow** column.

Full access
All incoming requests allowed. Set the **Default policy** to **Allow**.

To change the port number for a service, change the entry in the **Port** column for the given service. For example, to change the web server to port 8080 on the wireless port, enter 8080 in the WLS column on the Web Server row.

> **Warning**
>
> It is recommended to only enable services which are required for normal operation of the unit. If a service is required for configuration or testing only allow access when required then remove the access. This serves to improve security and avoid possible additional connections and resulting increase in data.

Click the Update button to save and commit changes or click the Reset button to clear the changes.

10.3 DoS Filters

10.3.1 Description

A denial of service attack (DoS attack) is an attempt to render a network device unavailable to intended users. The most common method of attack involves saturating the target device with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. The intention of DOS attacks is to cause the targeted device to reset or consume resources to such a level that it is unable to provide the intended service. A consequence of such an attack is that even if the device is able to handle the large number of communications requests, the bandwidth over the communications channel used for the attack may be completely consumed, potentially preventing legitimate connections to the targeted device.

The firewall has filters that can detect and drop packets that may be part of a Denial of Service (DOS) attack, for example, TCP packets with invalid header information. Options to enable and disable these filters can be found on DoS Filters page.

10.3.2 Enabling the Denial of Service filters

The Filter Description table provides a number of DOS filters, as shown in Fig. 10.4. The filters can be applied to packets received from the LAN port, the wireless port (WLS), and from any VPN tunnel by checking the boxes in the appropriate column.

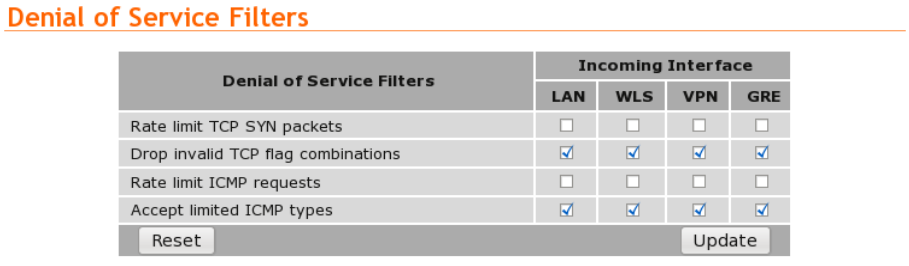


Fig. 10.4: Firewall DoS filter options

The function of each filter is described below:

Rate limit TCP SYN packets
This will limit the number of new TCP connection requests (SYN packets) allowed from the given interface. The rate will be limited to 5 per second.

Drop invalid TCP flag combinations
Some DOS attacks will send packets that present an invalid combination of TCP flags which may

cause problems for some operating systems. The filter will packets with invalid combinations received on the given interface.

Rate limit ICMP requests
This will limit the number of ICMP requests (for example, ping requests) allowed from the given interface. The rate will be limited to 5 per second.

Accept limited ICMP types
The types of ICMP packets that are accepted will be limited to types 0, 3, 8 and 11.

Click the Update button to save and commit changes or click the Reset button to clear the changes.

Warning

It is important to note that although the firewall will drop the packets as described the packets are still received over the WAN interface. This means that the WAN interface still may become saturated due to the number of packets received and there will possibly be excessive data charges. If an excessive number of packets are received the issue may need to be raised with the provider.

10.4 Custom Filters

10.4.1 Description

Custom Filters allow new rules to be added to the firewall to allow or deny specific packets. Packets can be matched based on which of the modem's network interfaces they arrive on or will leave on, the protocol, the source or destination address.

Some example custom filters are:

- A filter that only allows traffic from a particular host on the WAN to access through to the LAN ports.
- A filter that drops all traffic from a particular host on the WAN.

To select the Custom Filters page select *Firewall* → *Custom Filters*, a page similar to that shown in Fig. 10.5 will be displayed.

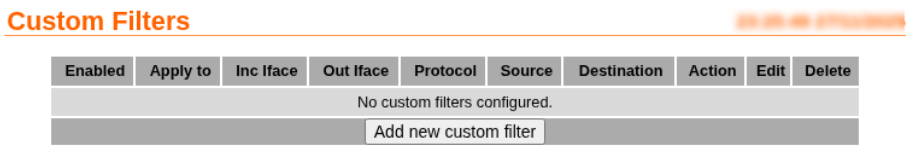


Fig. 10.5: Custom Filter main page with no filters configured

10.4.2 Custom filter options

To add a new custom filter click the Add new custom filter button, the custom filter options will be displayed as shown in Fig. 10.6. The same options page is displayed when a custom filter is edited by clicking the icon in the **Edit** column of the filter to be edited.

The following options can be set for each custom filter:

Enabled
Set the enabled check box to have the rule installed in the firewall. A rule can be temporarily disabled by un-checking this box.

Apply to
Custom filters can be applied at three separate points in the modem:

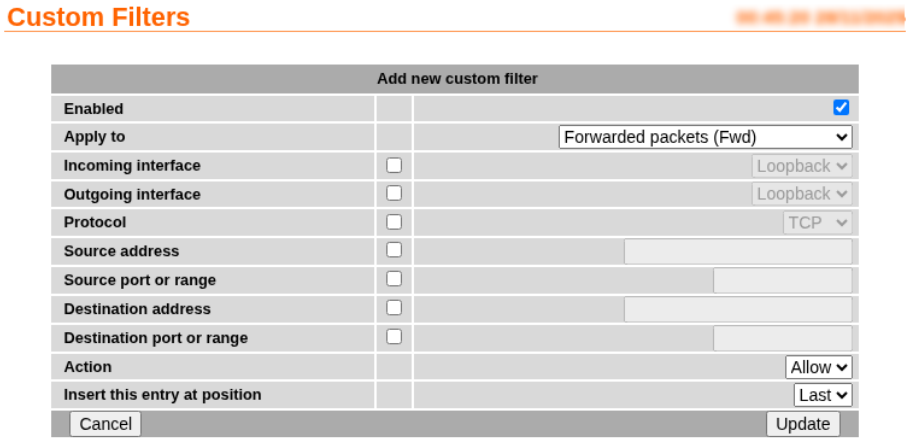


Fig. 10.6: Adding a new custom filter

Forwarded packets.
The filter will be applied to packets that are received from one network interface and then routed out another network interface.

Locally destined packets.
The filter will be applied to packets destined for the modem's internal services.

Locally generated packets.
The filter will be applied to packets generated by one of the modem's internal services.

Incoming interface
If selected, packets will be matched based on the network interface they have been received on. Note that this can't be applied to **Locally generated packets** as they have been generated by the modem itself.

Outgoing interface
If selected, packets will be matched based on the network interface they will be transmitted on. Note that this can't be applied to **Locally destined packets** as they will be received by the modem itself.

Protocol
If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address
If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the filter applied to them.

Source port or range
If selected, packets will be matched based on their TCP or UDP source port. Either an individual port (for example, 443) or a range of ports (80-143) can be entered.

Destination address
Similar to the **Source address**, but instead matching on the destination address.

Destination port or range
Similar to the **Source port or range,** but instead matching on the destination port.

Action
Determines what action on packets who meet all of the matching criteria for the filter. Options:

Deny
The packet will be dropped.

Allow
The packet will be passed.

Insert this entry at position
Determines where this entry will be inserted in the list of custom filters.

Click the Update button to save and commit changes or click the Cancel button to cancel the addition or edit.

10.4.3 Adding a new custom filter

From the main Custom Filters page click the **Add new custom filter** button. This will select the Add new custom filter page. An example of adding a new custom filter is shown in Fig. 10.7. In this example, a new filter is to be created to allow packets received via the wireless port, from IP address 112.112.112.112 and destined to the LAN network.

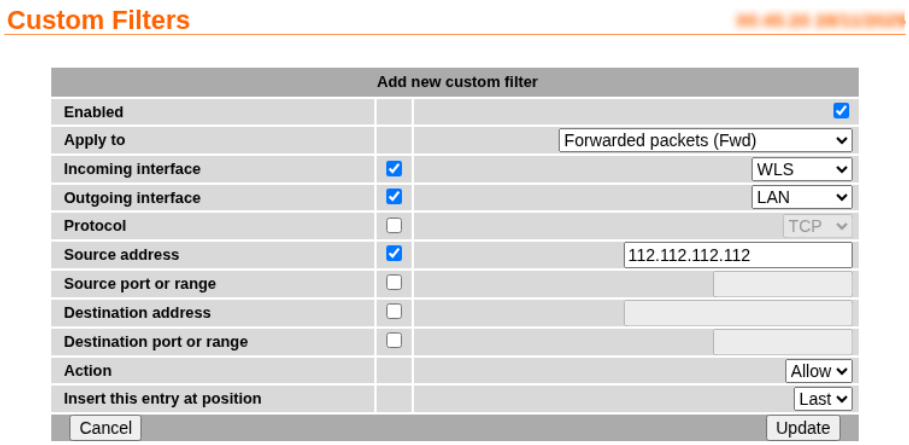


Fig. 10.7: Adding a new custom filter

It can be seen in the example that in the centre column, **Incoming interface**, **Outgoing interface** and **Source address** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

To save the new filter click the Update button. The main Custom Filter page will again be shown with the new filter listed, as shown in Fig. 10.8.

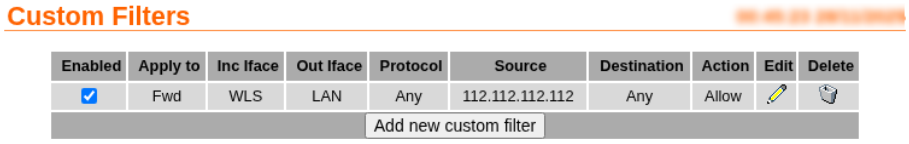


Fig. 10.8: The custom filter page with a single filter

To add a second filter again click the **Add new custom filter** button. In the example shown in Fig. 10.9, a custom filter is created which will deny packets received from the LAN port, from IP address 211.211.211.211 and destined to the wireless network. Again notice that in the centre column, **Incoming interface**, **Outgoing interface** and **Source address** are checked. This indicates these are the matching criteria that will be applied to packets. All criteria that are unchecked will be ignored.

To add the filter to the filters table click the Update button, the main page will again be shown with the new filter added, as seen in Fig. 10.10.

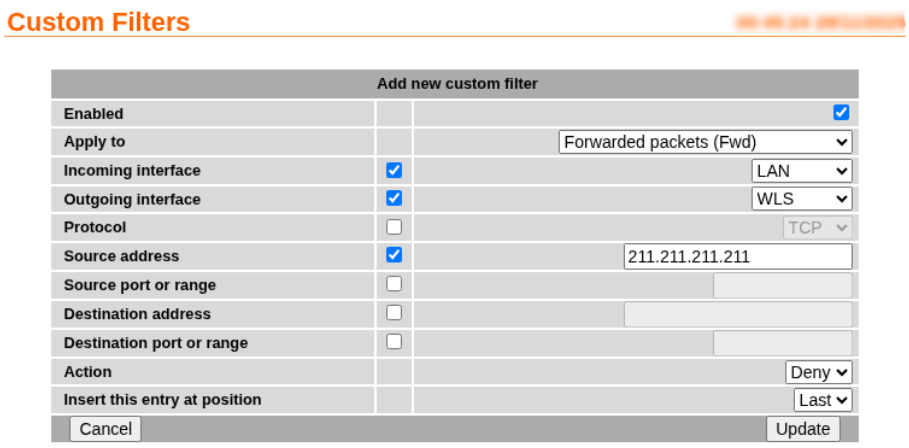


Fig. 10.9: Adding a new custom filter

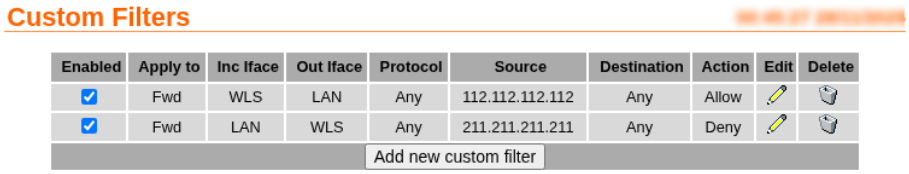


Fig. 10.10: The custom filter table with 2 filters

10.4.4 Editing a custom filter

A custom filter can be edited by clicking the  icon in the **Edit** column of the filter to be changed. Once clicked, the details of the filter will display in the same table as shown when adding a new filter.

As an example, to edit the second filter, click the  icon in the second row of the table. A page similar to the Add new filter page will be displayed, but now showing the details of filter 2. Changes that add protocol and port number matching to the criteria are shown in Fig. 10.11.

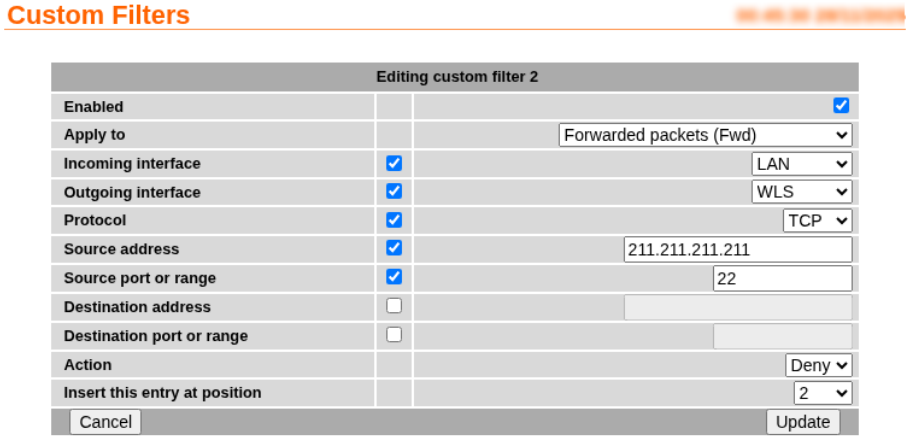


Fig. 10.11: Editing a custom filter

To save the changes click the Update button or to lose any changes click the Cancel button. The main page will again be displayed as shown in Fig. 10.12, with the changes for filter 2 added to the table.

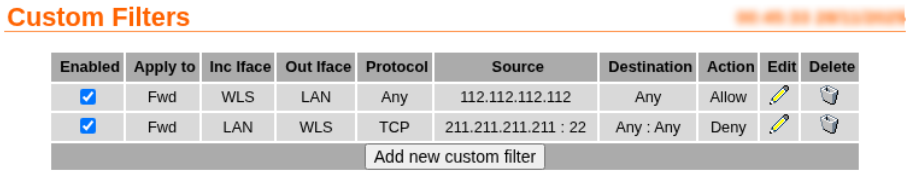


Fig. 10.12: The main custom filter table after editing filter 2

10.4.5 Deleting a custom filter

A custom filter can be deleted by clicking the icon in the **Delete** column of the filter to be deleted. A warning box will be displayed. Click **OK** to confirm the deletion or **Cancel** to prevent the filter from being deleted.

For example, to delete filter 2 from the table shown in Fig. 10.12, click the icon in row 2 of the table. A warning box will now be displayed, as shown in Fig. 10.13. Click **OK** to confirm.

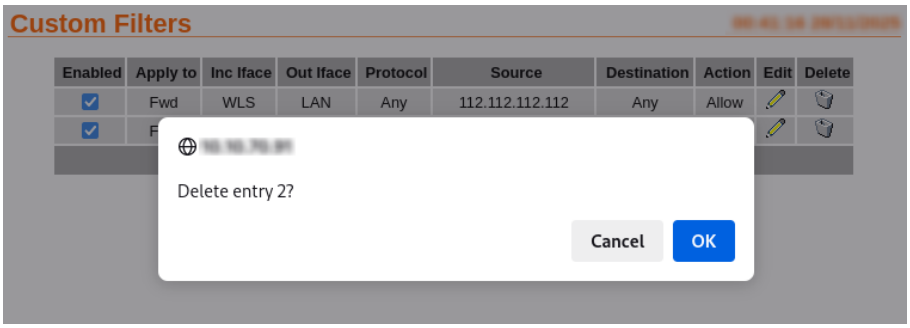


Fig. 10.13: Deleting a custom filter

The filter table will be displayed with filter removed, as shown in Fig. 10.14.

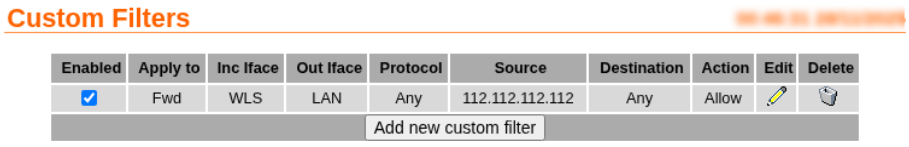


Fig. 10.14: Custom filter table with filter 2 removed

10.5 Port Forwarding

10.5.1 Description

Port forwarding rules alter the destination address (and optionally the destination port) of packets received on the WAN or VPN interfaces of the modem. Port forwards can be used to forward specific services (e.g. HTTP) to a private machine on the LAN network without needing to expose the entire private machine to the public network.

To access the port forward configuration page, select *Firewall → Port Forwards*, a page similar to that shown in Fig. 10.15 will be displayed.

10.5.2 Port forward options

To add a new port forward click the Add new port forward button, the port forward options will be displayed as shown in Fig. 10.16. The same options page is displayed when a port forward is edited by clicking the icon in the **Edit** column of the port forward rule to be edited.

Fig. 10.15: Port forward page with no port forwards configured

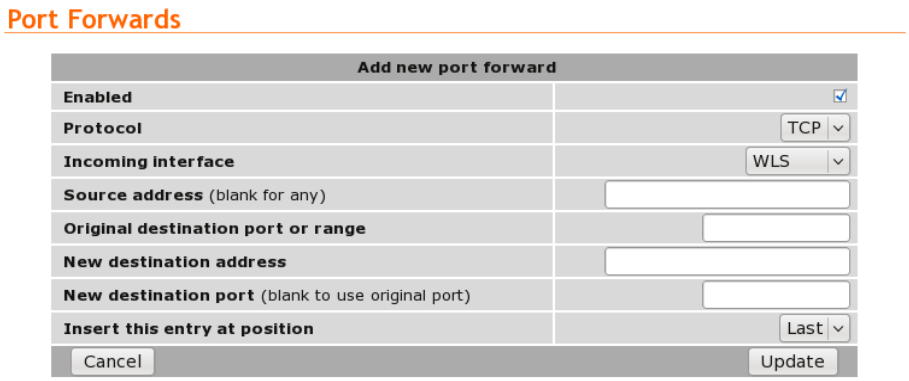


Fig. 10.16: Page to add a Port forward

The following options can be set for each port forward:

Enabled
Set the enabled check box to have the rule installed in the firewall. A rule can be temporarily disabled by un-checking this box.

Protocol
The modem is able to forward TCP, UDP, GRE, ESP and AH. Most forwards will be either TCP or UDP. Select the appropriate protocol from the list.

Incoming interface
Select the interface that the packets to be forwarded on will arrive (in this case, WLS, the wireless port, is selected).

Source address
For greater security, the source addresses that the forward will be applied to can be limited. In this field, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered.

Original destination port or range
This is the port number (80 in the example) but can also be a range (entered as, for example, 120-150) that the firewall will match on to forward to the new destination address.

New destination address
This is the IP address of the server to forward to (10.10.10.50 in the example).

New destination port
In addition to changing the destination address, it is also possible to change the destination port. To do so, enter the port in this field. This field can be left blank to keep the port the same.

Insert this entry at position
Determines where this entry will be inserted in the list of port forwards.

Click the Update button to save and commit changes or click the Cancel button to cancel the addition or edit.

10.5.3 Adding a new port forward

From the main port forwards page, click the Add new port forward button. This will select the Add new port forward page. An example of adding a new port forward is shown in Fig. 10.17. In this example a new port forward is created to forward from port 80 of the wireless port to a HTTP server at address 10.10.10.50.

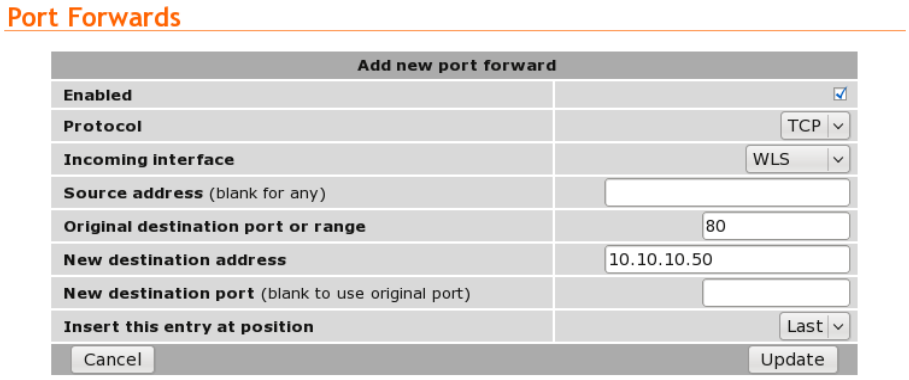


Fig. 10.17: Adding a port forward

Click the Update button to save and commit the new port forward. The port forward table will be updated to include the new port forward as shown in Fig. 10.18.

Fig. 10.18: The port forward page with a single port forward

To add a second port forward click the Add new port forward button. In the example shown in Fig. 10.19, a port forward is created which forward packets received for IP address 112.112.112.112 on port 2200 of the wireless port to LAN IP address 10.10.10.72.

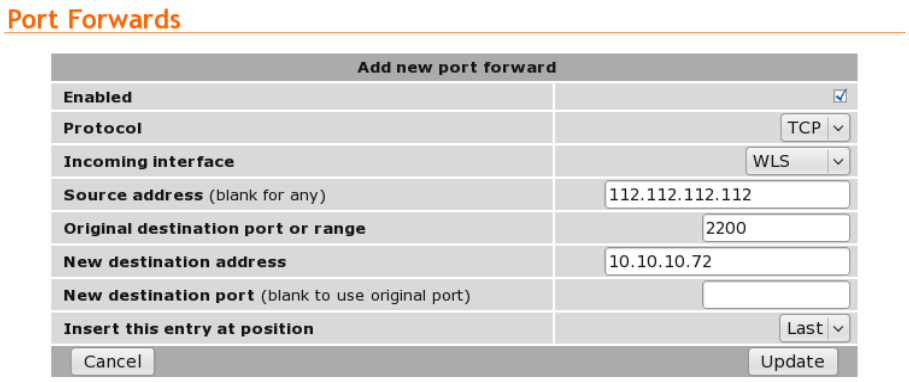


Fig. 10.19: Adding a second port forward

To add the new port forward to the port forward table click the Update button. The main page will again be shown with the new port forward added, as seen in Fig. 10.20.

Fig. 10.20: The port forward page with a two port forwards

10.5.4 Editing a port forward

A port forward can be edited by clicking the icon in the **Edit** column of the port forward to be changed. Once clicked, the details of the port forward will be displayed in the same table as when creating a new port forward.

As an example, to edit the second port forward in the port forward table, click the icon in the second row of the table. A page similar to the Add new port forward page will be displayed but will show the details of port forward 2. Changes were made so the destination is now port 22 as shown in Fig. 10.21.

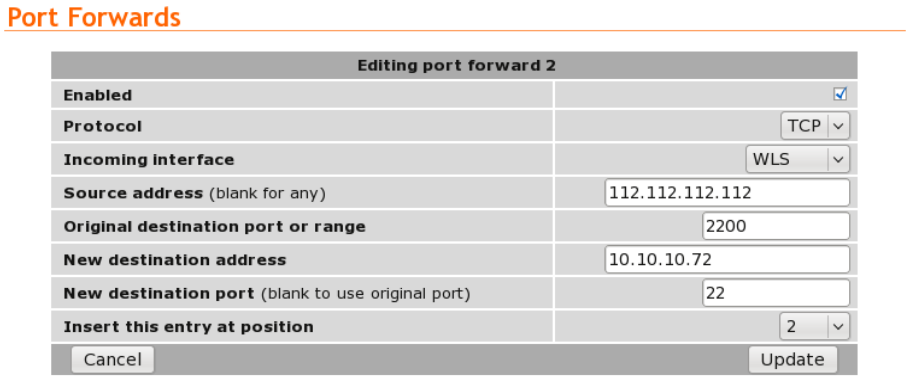


Fig. 10.21: Editing a port forward

To save the changes, click the Update button or to lose changes click the Cancel button. The main page will again be displayed as shown in Fig. 10.22, with the changes for port forward 2 added to the table.

Fig. 10.22: Main port forward page with revised port forward

10.5.5 Deleting a port forward

A port forward can be deleted by clicking the icon in the **Delete** column of the forward to be deleted. A warning box will be displayed. Click **OK** to confirm the deletion.

For example, to delete port forward 2 from the table shown in Fig. 10.22, click the icon in row 2 of the table. A warning box will now be displayed as shown in Fig. 10.23. Click the OK button.

The port forward table will be displayed with the port forward removed, as shown in Fig. 10.24.

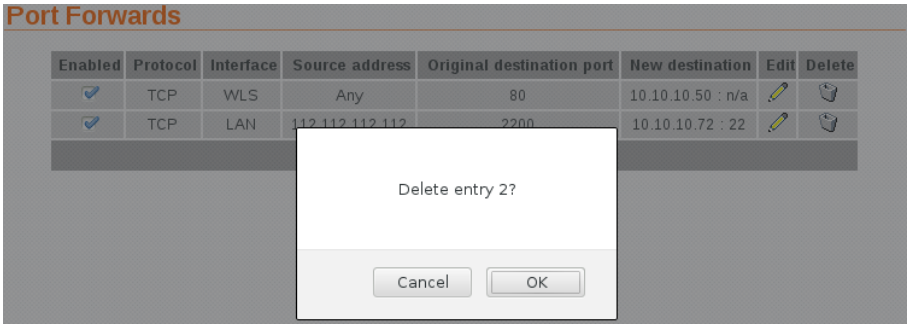


Fig. 10.23: Deleting a port forward

Fig. 10.24: Port forward table of deleting a port forward

10.6 Custom NAT

10.6.1 Description

Custom NAT allows new rules to be added to the firewall to carry out Network Address Translation (NAT) that is different to the usual NAT provided by the firewall. Packets can be matched based on which of the modem's network interfaces they arrive on or will leave on, the protocol, the source or destination address. The packets can have Source-NAT (SNAT) applied, where the source address is altered, or Destination-NAT (DNAT) applied, where the destination address is altered.

Some example custom NATs are:

- Source-NAT on all packets being transmitted out a VPN tunnel.
- Destination-NAT to redirect packets to a host on the LAN.

To access the Custom NAT configuration page, select *Firewall* → *Custom NAT*, a page similar to that shown in Fig. 10.25 will be displayed.

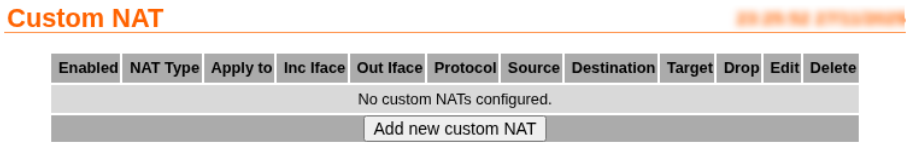


Fig. 10.25: Main custom NAT page, with no custom NAT entries in the table

10.6.2 Custom NAT options

To add a custom NAT rule click the Add new custom NAT button, the custom NAT options will be displayed as shown in Fig. 10.26. The same options page is displayed when a custom NAT is edited by clicking the  icon in the **Edit** column of the NAT rule to be edited.

The following options can be set for each custom NAT:

Enabled
: Set the enabled check box to have the rule installed in the firewall. A rule can be temporarily disabled by un-checking this box.

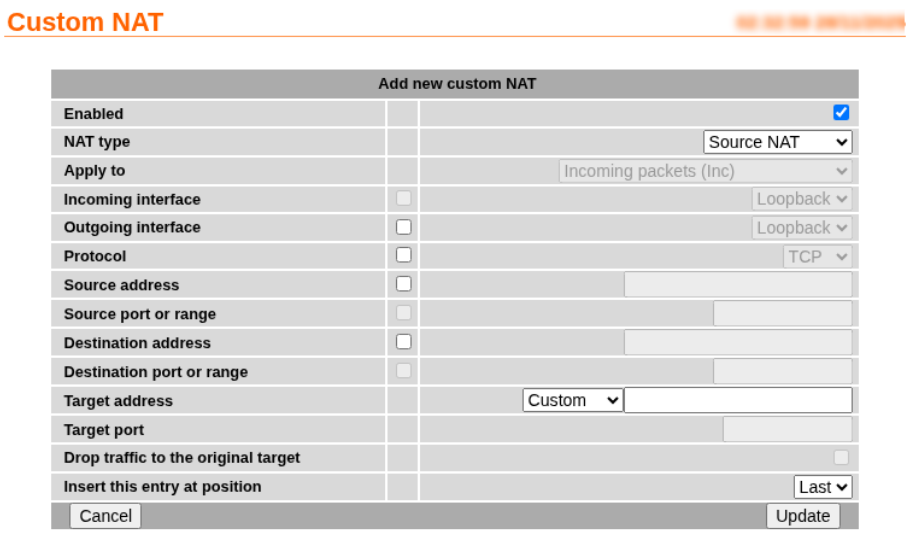


Fig. 10.26: Add new Custom NAT page

NAT Type
Determines the type of NAT the entry will perform. Options:

Source NAT
Source NAT changes the source address in IP packet and may also change the source port.

Destination NAT
Destination NAT changes the destination address in IP packet and may also change the destina tion port.

1:1
Provides a one-to-one translation of IP addresses. This type of NAT is also known as Basic NAT

Apply to
When entering a destination NAT, there are two places the NAT can be applied:

Incoming packets
The rule will be applied to packets received from the modem's network interfaces.

Locally generated packets
The rule will be applied to packets generated by an internal service.

Incoming interface
If selected, packets will be matched based on the network interface they have been received on. Note that this can only be applied to a **Destination NAT** on **Incoming packets**.

Outgoing interface
If selected, packets will be matched based on the network interface they will be transmitted on. Note that this can only be applied to a **Source NAT.**

Protocol
If selected, packets will be matched based on their protocol type. Note that if you wish to match on source or destination ports, the protocol must be set to **TCP** or **UDP**.

Source address
If selected, either a single address (for example, 172.16.1.132) or a subnet range (for example, 172.16.0.0/24) can be entered. Only packets matching this source address will have the filter applied to them.

Source port or range
If selected, packets will be matched based on their TCP or UDP source port. Either an individual

port (for example, 443) or a range of ports (80-143) can be entered.

Destination address
Similar to the **Source address**, but instead matching on the destination address.

Destination port or range
Similar to the **Source port or range,** but instead matching on the destination port.

Target address
This is the address that the NAT rule will apply to packets. When set to **Custom**, any IP address can be entered in the text box. If an interface is selected from the drop-down box, the current address of that interface will be applied to packets.

Target port
For rules that specify either the TCP or UDP protocol, it is possible to also alter the port number. If no change of port number is desired, this field can be left blank.

Insert this entry at position
Determines where this entry will be inserted in the list of custom NAT rules.

Click the Update button to save and commit changes or click the Cancel button to cancel the addition or edit.

10.6.3 Adding a new custom NAT

From the main custom NAT page click the Add new custom NAT button. This will select the Add new custom NAT page. An example of adding a new custom NAT is shown in Fig. 10.27. In this example, a new custom NAT is created which will source NAT packets outgoing on the SSL VPN interface to the IP address of the SSL VPN.

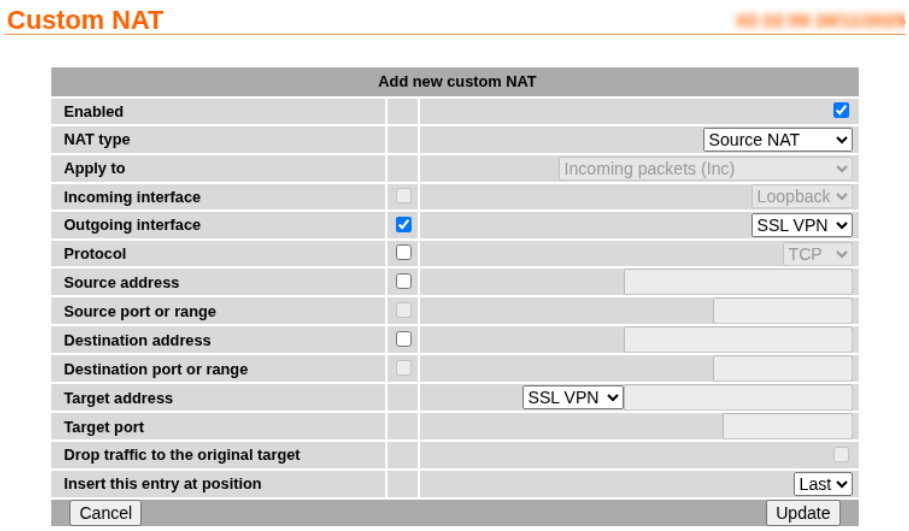


Fig. 10.27: Adding a custom NAT

It can be seen in the example that in the centre column only **Outgoing interface** is checked. This indicates these are the matching criteria that will be applied to packets. In this case, all packets outgoing on the SSL VPN will be source NAT'd.

Click the Update button to save and commit new custom NAT rule. The custom NAT table will be updated to include the new custom NAT as shown in Fig. 10.28.

To add a second custom NAT again click the Add new custom NAT button. In the example shown in Fig. 10.29, a destination NAT is created for packets destined for the wireless port.

To add the new custom NAT click the Update button. The main page will again be shown with the new custom NAT added, as seen in Fig. 10.30.

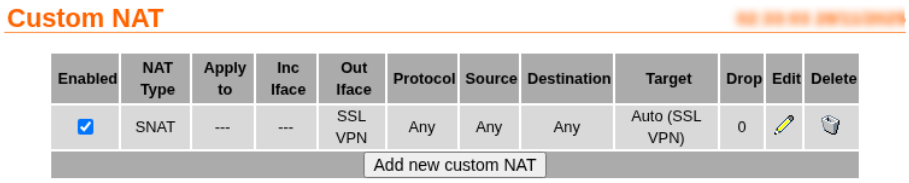


Fig. 10.28: Main custom NAT page showing new custom NAT added to the table

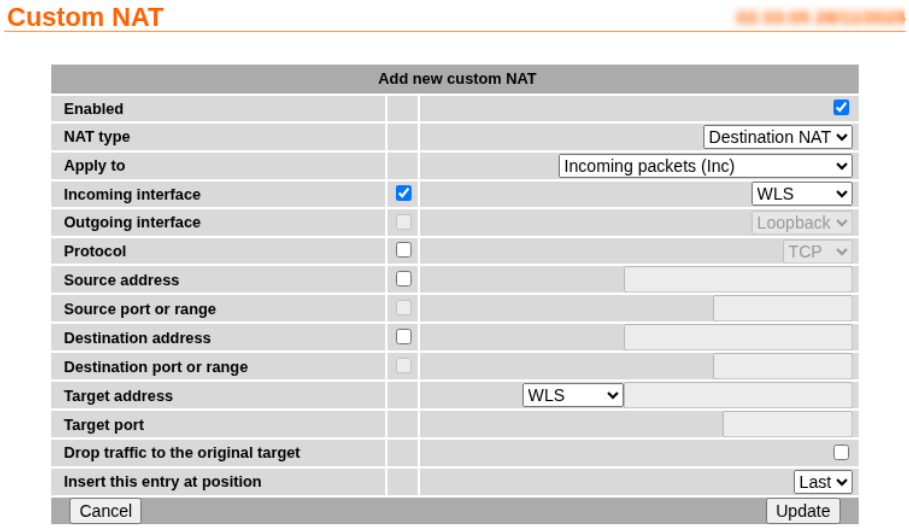


Fig. 10.29: Adding a custom NAT

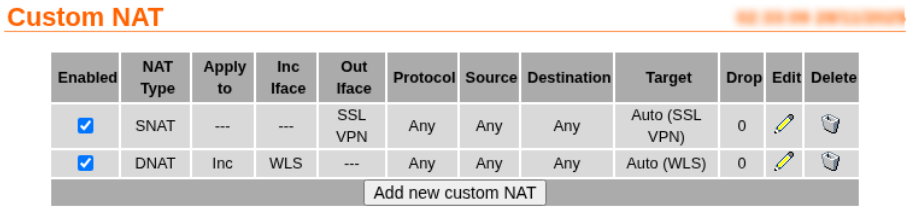


Fig. 10.30: Main custom NAT page showing new custom NAT added to the table

10.6.4 Editing a custom NAT

A custom NAT can be edited by clicking the icon in the Edit column of the filter to be changed. Once clicked, the details of the custom NAT will be displayed in the same table as when creating a new custom NAT.

As an example, to edit the second custom NAT in the Custom NAT table shown in Fig. 10.30, click the icon in the second row of the table, A page similar to the new custom NAT page will be displayed but with the details of custom NAT 2. To set the protocol for the custom NAT to be UDP, changes were made as shown in Fig. 10.31.

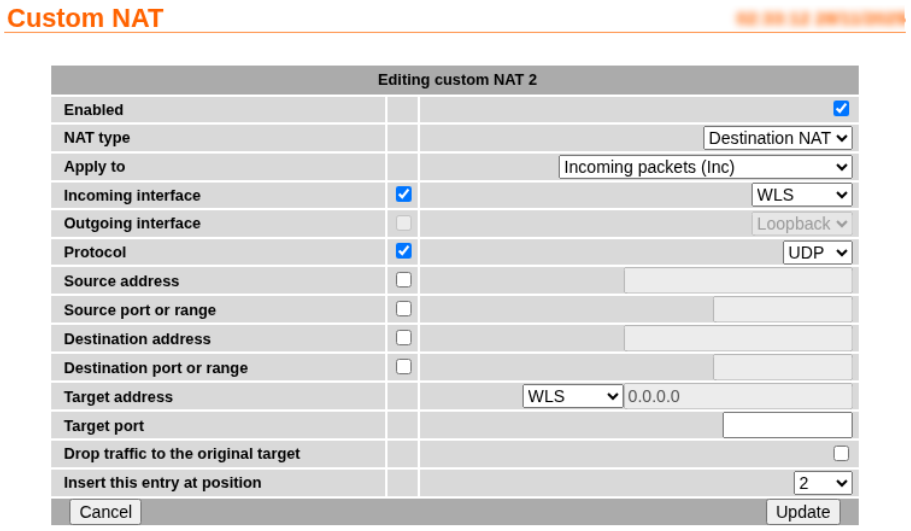


Fig. 10.31: Editing a custom NAT

To save the changes click the Update button or to lose the changes click the Cancel button. The main page will again be displayed as shown in Fig. 10.32, with the changes for custom NAT 2 added to the table.

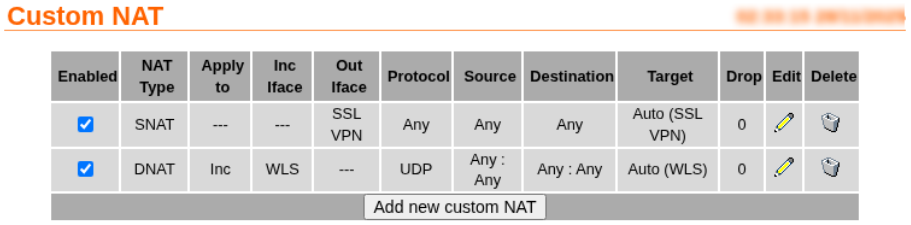


Fig. 10.32: Main custom NAT page with revised custom NAT 2

10.6.5 Deleting a custom NAT

A custom NAT can be deleted by clicking the icon in the **Delete** column of the NAT to be deleted. A warning box will be displayed. Click **OK** to confirm the deletion.

For example, to delete custom NAT 2 from the table shown in Fig. 10.32, click the icon in row 2 of the table. A warning box will now be displayed as shown in Fig. 10.33. Click the OK button.

The custom NAT table will be displayed with the custom NAT removed, as shown in Fig. 10.34.

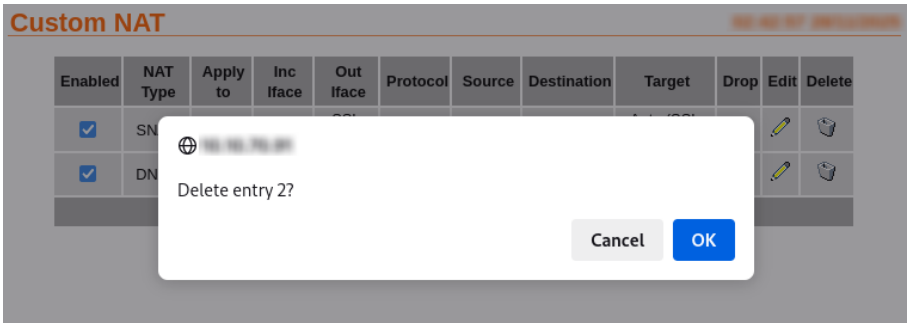


Fig. 10.33: Deleting a custom NAT

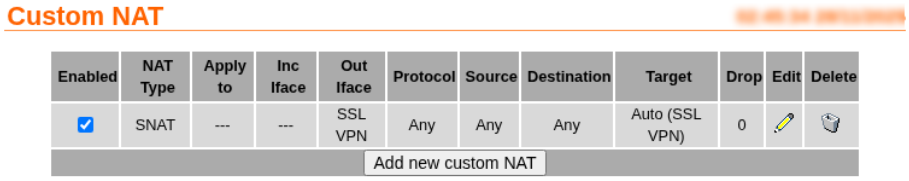


Fig. 10.34: Custom NAT table after deleting a custom NAT

10.7 MAC Address Filtering

10.7.1 Description

The firewall supports Media Access Control (MAC) address filtering. A unique MAC address is assigned to every Ethernet device, this address can be filtered to either allow or deny a device access to a device or network.

> **Warning**
>
> While providing a network with a level of protection, MAC Filtering can be circumvented by scanning the network for a valid MAC and then changing the MAC address of the attacker's machine to a validated one. For this reason if access to the LAN interface is to be restricted MAC address filtering should not be used as the only form of security.

To access the MAC Address Filters configuration page, select *Firewall* → *MAC Filters*, a page similar to that shown in Fig. 10.35 will be displayed.

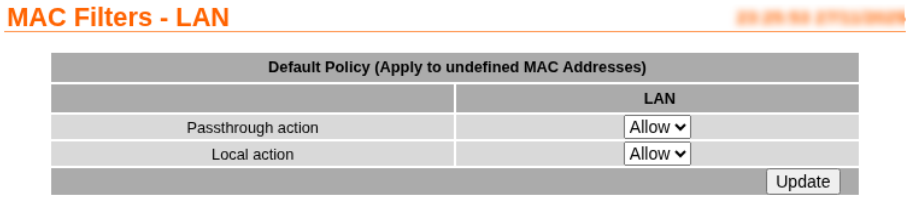


Fig. 10.35: MAC Address filters main page.

10.7.2 Default policy

The default policy sets the action to be taken for all MAC addresses not listed in the MAC address table. The options for this are *Allow* and *Deny*. If the default policy is to be set to Deny it is recommended this is done after the Allow rules have been added so as to prevent accidental lock-out.

Warning

Care should be taken when configuring MAC Filters to ensure the computer being used to configure the device is not denied access if as likely it is connected to the LAN interface. When changing filters it is recommended to first add a specific filter to allow access to the computer being used for configuration. If after configuration is complete the rule is no longer required it can be deleted.

If the computer used for configuration is denied access then it will be necessary to perform a factory reset of the device. This will clear all the configuration settings to the factory default settings and the LAN ports will be enabled.

Tip

If the access via the LAN interface is restricted then access to the web configuration pages may be available via the wireless interface if the firewall settings allow access.

Passthrough action
Action for packets destined for the WAN interface. Options:

Allow
All non-matching MAC addresses accepted.

Deny
All non-matching MAC addresses dropped.

Local action
Action for packets destined for a service on the device. Options:

Allow
All non-matching MAC addresses accepted.

Deny
All non-matching MAC addresses dropped.

Click the Update button to save and commit changes.

10.7.3 Adding a MAC Filter

To add a MAC filter click the Add new MAC filter button, the MAC filter options will be displayed as shown in Fig. 10.36.

The same options page is displayed when a MAC filter is edited by clicking the  icon in the **Edit** column of the MAC filter to be edited.

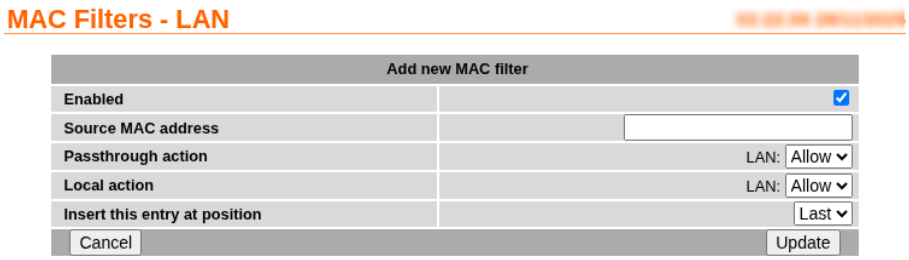


Fig. 10.36: Adding a MAC address filter.

The options are:

Enabled
Set to make active the filter. A filter can be disabled by un-checking this box.

Source MAC address
The MAC address on which the filter will be applied.

Passthrough Action
The action to be applied for pass-through, the options are:

Allow
Packets with matching MAC address will be pass-through to the WAN interface.

Deny
Packets with matching MAC will be denied access to the WAN interface.

Local Action
The action to be applied for local services the options are:

Allow
Packets with matching MAC address will be passed to the local services.

Deny
Packets with matching MAC will be denied access to the local services.

Insert this entry at position
Determines where this entry will be inserted in the list of MAC address filters.

Click the Update button to save and commit changes.

10.7.4 Example MAC Address Filters

On the MAC Address Filter page click the Add new MAC filter button. This will select the Add new MAC Filter page. In this example, shown in Fig. 10.37 a new MAC filter will be added to allow MAC address 00:11:22:33:44:55 both pass-through and local access.

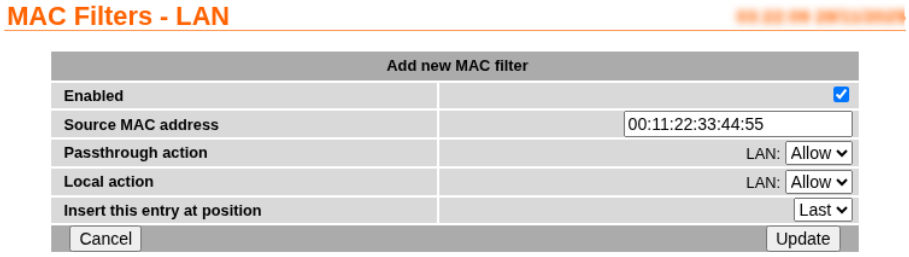


Fig. 10.37: Example of adding an MAC filter.

Once the details have been entered click the Update button to save the new MAC filter.

The MAC filter table will be updated to include the MAC filter rule as shown in Fig. 10.38.

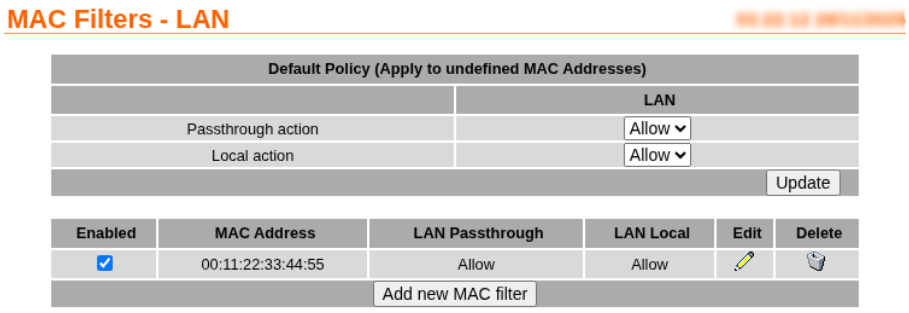


Fig. 10.38: MAC filter table with new rule added.

To add a second MAC filter again click the Add new MAC filter button. In the example, shown in Fig. 10.39, a MAC address filter has been added to allow MAC address 55:44:33:22:11:00 again with pass-through and local access.

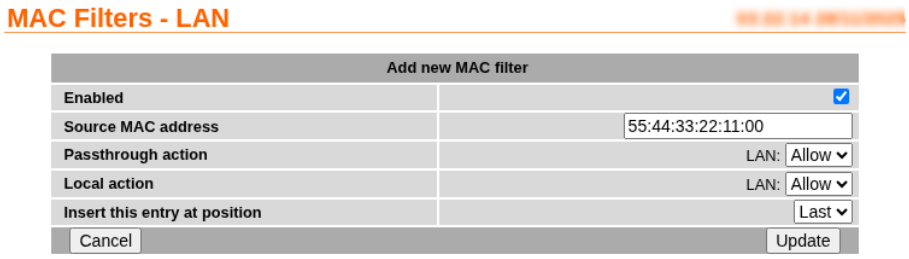


Fig. 10.39: Adding a MAC Filter rule.

To add the new MAC filter click the Update button. The main page will again be shown with the new MAC filter rule added, as seen in Fig. 10.40.

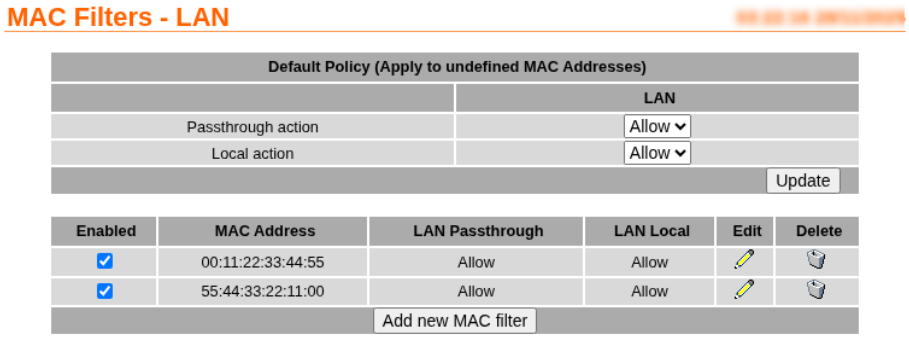


Fig. 10.40: MAC address table with new rule added

10.7.5 Editing a MAC Filter

A MAC Filter can be edited by clicking the icon in the **Edit** column of the filter to be changed. Once clicked, the details of the MAC Filter will be displayed in the same way as when creating a new MAC Filter.

As an example, to edit the second MAC Filter in the MAC Filter table shown in Fig. 10.40, click the icon in the second row of the table, A page similar to the new MAC Filter page will be displayed but containing the details of MAC Filter 2. To change the Local Action for this rule to Deny, changes were made as shown in Fig. 10.41.

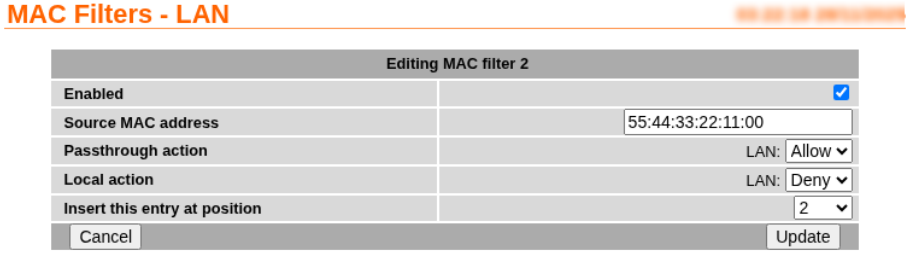


Fig. 10.41: Editing a MAC Filter

To save the changes click the Update button or to lose the changes click the Cancel button. The main page will again be displayed as shown in Fig. 10.42, with the changes for MAC Filter 2 added to the table.

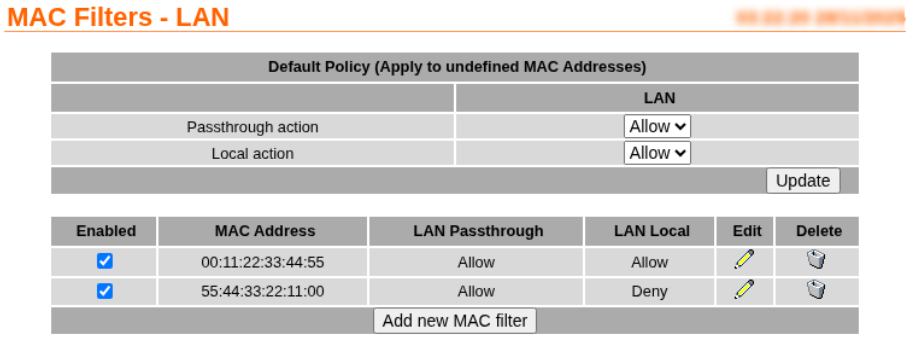


Fig. 10.42: MAC Filter table after changes to MAC filter 2.

10.7.6 Changing the default Policy

In the previous example the second MAC address filter denied access to the local services, however the default policy is to allow access to all MAC addressed which means the deny rule will not work. In order to correct this set the default action will need to change to Deny. In addition the first rule is an allow rule, so in order for this rule to be effective the default pass-through also needs to be set to Deny. This shown in Fig. 10.43.

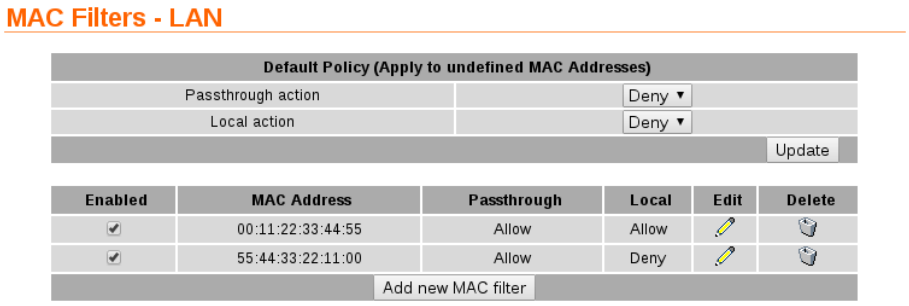


Fig. 10.43: MAC Filter page with default action set to deny.

10.7.7 Deleting an MAC Address Filter

A MAC Filter can be deleted by clicking the icon in the **Delete** column of the MAC Filter to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion.

For example, if it were decided not to allow pass-through in rule 2 the rule could be changed or the same result could be achieved by removing the rule. To delete MAC Filter 2 from the table shown in Fig. 10.43, click the icon in row 2 of the table. A warning box will now be displayed as shown in Fig. 10.44. Click the OK button.

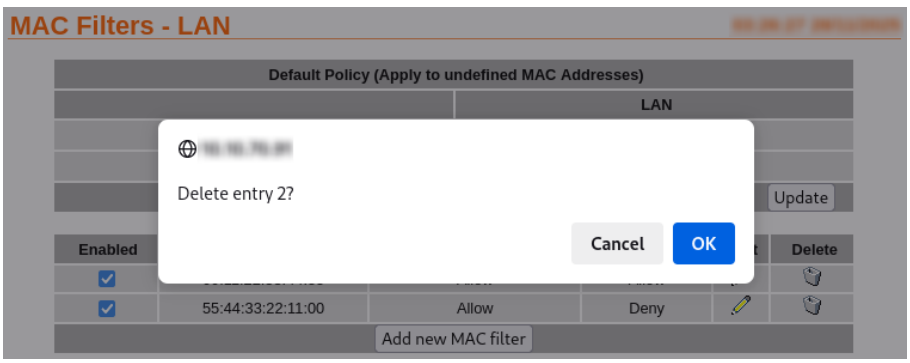


Fig. 10.44: Deleting a MAC Filter.

The MAC Filter table will be updated with the MAC Filter removed, as shown in Fig. 10.45.

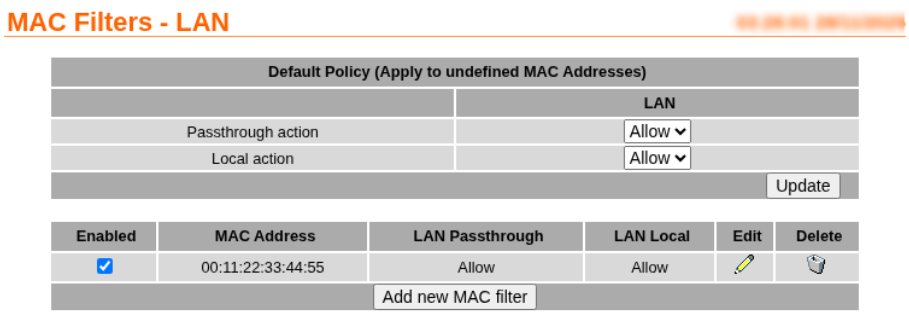


Fig. 10.45: MAC Filter table after deleting a MAC Filter.

CHAPTER

ELEVEN

VIRTUAL PRIVATE NETWORK (VPN)

A virtual private network (VPN) is a communications network tunnelled through another, usually insecure network. Generally the secured communications network is tunnelled through the wireless interface and then over the Internet or private network to a VPN-capable router or server. Support is provided for IPsec, SSL and PPTP/L2TP based VPNs and multiple VPN tunnels can be configured to operate simultaneously.

The main VPN page is accessed by clicking *VPN* on the main menu, the page displayed will be similar that shown in Fig. 11.1.

Fig. 11.1: The main VPN page.

11.1 Internet Protocol Security (IPsec) VPN

Internet Protocol Security (IPsec) is a suite of standards and protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. Also included within IPsec are protocols for cryptographic key establishment. IPsec protocols operate at the network layer (layer 3 of the OSI model). This means that it can be used for protecting layer 4 protocols, including both TCP and UDP, the most commonly used transport layer protocols. Using strong encryption and public key cryptography IPsec can secure data links over public networks which would otherwise be insecure.

IPsec is a framework which is built in to various security products from companies such as Cisco and Juniper to provide end-to-end security. IPsec functionality has been tested for interoperability with the Cisco implementation of IPsec known as Cisco IOS IPsec.

11.1.1 General IPsec configuration

To access the IPsec VPN configuration page click *VPN* → *IPsec* the page shown in Fig. 11.2 will be displayed. The page contains general IPsec configuration options at the top and a list of configured tunnels at the bottom.

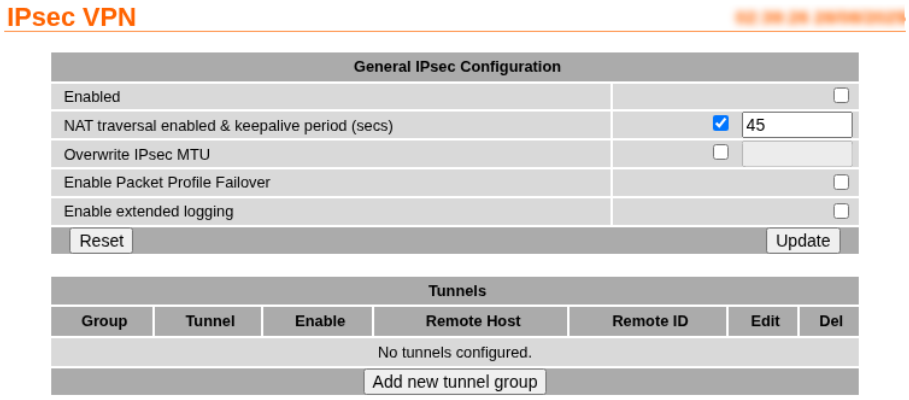


Fig. 11.2: IPsec based VPN main page.

The first table contains the **General IPsec configuration** settings. These will apply to all configured IPsec tunnels. The options are:

Enabled
: Check the box to enable the IPsec VPN application. Tunnels must be configured and enabled for this to do anything. Default is disabled.

NAT traversal enabled & keepalive period (secs)
: Check box to enable NAT Traversal and set the keepalive time.

  NAT Traversal
  : When passing through a Network Address Translator (NAT) an IP packet is modified in such a way that is incompatible with Internet Protocol Security (IPsec). NAT-Traversal protects the original IPsec encoded packet by encapsulating it within another layer of UDP and IP headers. If the wireless interface is allocated a dynamic and private IP address then the connection to the Internet will be via a Network Address Translator (NAT). This will require the use of NAT-Traversal for IPsec to establish a connection.

  Keepalive Period
  : NAT keepalives are used to keep the dynamic NAT mapping alive during a connection between two peers. NAT keepalives are UDP packets with an unencrypted payload of 1 byte. Although similar to dead peer detection (DPD) and IKEv2 Liveness keepalives, NAT keepalives are different. DPD and Liveness keepalives are used to detect peer status, while NAT keepalives are sent if the IPSec entity did not send or receive a packet in a specified period of time.

Overwrite IPsec MTU
: The Maximum Transmission Unit (MTU) is the size (in bytes) of the largest packet which can be sent over the IPsec tunnel. Leave the checkbox un-checked and the value blank to use the default setting. To change the MTU check the checkbox and enter the value.

Enable Packet Profile Failover
: Check to enable packet profile failover. When enabled and a secondary APN is configured in the wireless settings, the system can automatically failover to the secondary APN if the primary connection fails.

Enable extended logging
: Check to enable extended logging for IPsec. This option is useful if connection problems are encountered.

Click the Update button to save and commit changes.

The second table shows a summary of all configured tunnels. The next section details adding tunnels.

11.1.2 Adding an IPsec tunnel

To add an IPsec tunnel click the Add new tunnel group button. This will display the first of several pages used to configure the IPsec VPN tunnel. The first page is the Tunnel Configuration shown in Fig. 11.3.

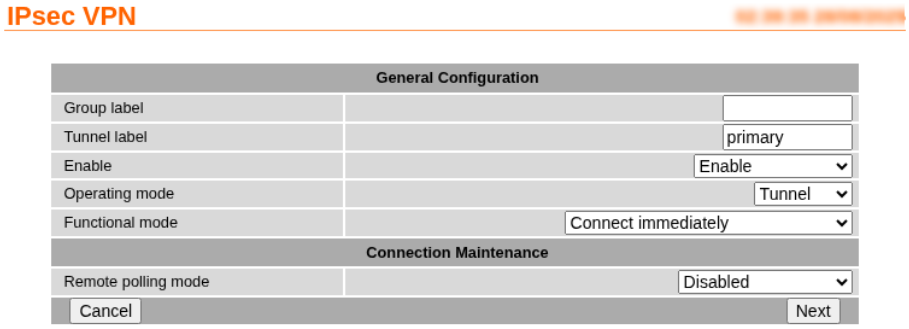


Fig. 11.3: IPsec tunnel configuration.

General Configuration

IPsec general configuration is the first stage in adding a new IPsec tunnel. This is the general configuration for the tunnel that is currently being configured. Not to be confused with the global general IPsec configuration that was previously mentioned. The options are as follows:

Group_label

Provide a label for the tunnel group. This is used as a reference and is particularly useful when more than one tunnel is configured. This label is required even if there is only 1 tunnel in the group. Each group label must be unique.

Tunnel label

Set the label or name for the tunnel within the group. This is used to distinguish between tunnels, for example 'primary' and 'secondary'. Each tunnel name should be unique within the group.

Enable

Select whether the tunnel should be allowed to start. Options are:

Disable

Don't start up this tunnel

Enable

Start up the tunnel. Note that if this tunnel is configured to use the WAN interface in any way, that this tunnel will not start up until the WAN interface has been successfully brought up.

Enable On VRRP

Start up the tunnel when the unit becomes a VRRP master. This requires VRRP to be running on the device to work properly.

Operating mode

Select the operating mode of the IPsec tunnel from the following options:

Tunnel

Tunnel mode encapsulates the entire IP packet to provide a secure connection between two gateways. In tunnel mode the payload, the header and the routing information are all encrypted, and then encapsulated into a new IP packet. This mode is generally the more common method used to create a VPN.

Transport

Transport mode provides a secure connection between two hosts. Only the payload of the IP packet is encrypted.

Functional mode
Select the functional mode of the IPsec tunnel from the following options:

Connect immediately
The tunnel will be initiated, that is it will attempt to establish a connection with a remote responder. Both ends of the connection acting as initiators can technically work, but will show odd and inconsistent behaviour.

Responder or Connect on demand
Wait for and respond to incoming connections. If there is no active connection running and traffic tries to go to anything that would be accessible if the tunnel was up, then attempt to bring the tunnel up.

Connection Maintenance
IPsec tunnel connection maintenance options. When enabled, this is used to ensure that traffic is going over the IPsec tunnel properly, and will restart tunnels if it isn't. The options are:

Remote polling mode

Disabled
No remote polling.

Poll at fixed interval
Enable polling that will occur at a regular interval, until no responses are received. More configuration options will appear when this mode is selected. The options are:

Poll period (secs, min 15)
Specify the time interval, in seconds, between polls. Minimum value of 15 seconds.

Retry period (secs, min 15, max poll period)
Check to enable and specify the time, in seconds, to retry the poll after a failed poll has occurred. Minimum value is 15 seconds. Max value is the value configured for the poll period.

Failed establishment polls before restarting the connection
Specify the number of failed establishment polls to declare the connection down and restart the establishment process. Polling will only occur on the establishment of the connection to ensure it is running as intended.

Failed polls before restarting the connection
Specify the number of failed polls to declare the connection down and to restart the establishment process. This value must be 1 or greater.

Poll Type
Specify the poll type to use. The options are:

Ping (ICMP)
Use pings to poll the specified address

TCP Socket
Establish a TCP socket to the specified address and port number. The TCP connection will be terminated as soon as it is successfully opened.

Source address
Check to enable a source address. Source address configures a source address to be used when polling remote the address. The configured source address must be a valid address for the poll to use, not just a valid ip address, but the source address must make sense for the interface. This is not normally needed, and is normally used when there are multiple potential source addresses for the remote poller to use, which is dependent on the tunnel mappings configured.

Poll address
Specify the remote IP address to poll. It is recommended for this to be something that can only be accessed once the tunnel is up. If the poll type is TCP Socket the port number should also be included in this field. It should be in the format <IP>:<port>

Once configuration is complete on this page click the Next button to move to the next page.

Physical Layer Configuration

The second page is the Physical Layer Configuration page, the options on the page will depend on the functional mode selected on the last page ("Connect immediately" or "Responder or Connect on demand"). Fig. 11.4 shows the options for the initiator mode, while Fig. 11.5 shows the options for the responder mode.

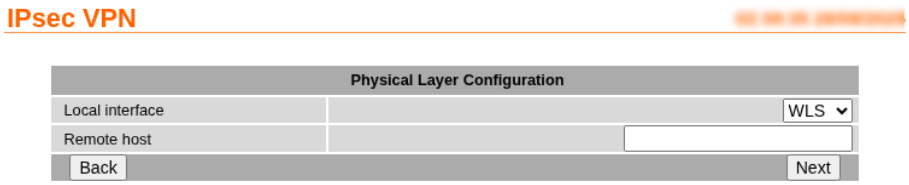


Fig. 11.4: IPsec physical configuration initiator mode.

The options for physical layer configuration, when configured as an initiator are as follows:

Local interface
Select the interface over which to create the tunnel. The drop-down box will show all of the available options for the device. Possible options are:

WLS
The wireless interface.

xDSL
The DSL interface.

LAN
The local Ethernet interface.

LAN2
The secondary local Ethernet interface.

> **Note**
> The LAN2 option will only appear if the modem has "independent LAN ports" enabled on the LAN network page, making LAN2 a valid option.

If LAN or LAN2 is selected, the additional options will appear:

Local Gateway (Nexthop)
Enter the gateway or next hop address. Refer to Fig. 11.6 as an example of the responder page with the local interface set to LAN.

Remote host
Provide the address of the remote host to which a connection should be established.

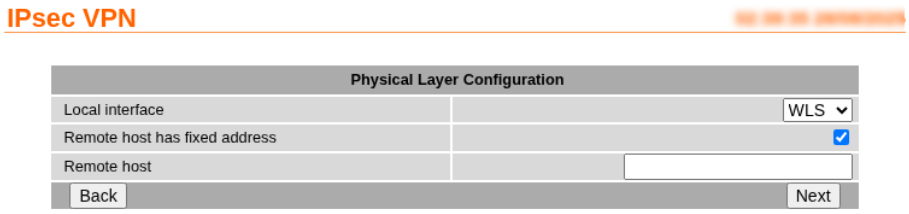


Fig. 11.5: IPsec physical configuration responder mode.

The options for physical layer configuration when configured as a responder are as follows:

Local interface
Select the interface over which to create the tunnel. The drop-down box will show all of the available options for the device. Possible options are:

WLS
The wireless interface.

xDSL
The DSL interface

LAN
The local Ethernet interface.

LAN2
The secondary local Ethernet interface.

> **Note**
>
> The LAN2 option will only appear if the modem has "independent LAN ports" enabled on the LAN network page, making LAN2 a valid option.

If LAN or LAN2 is selected, the additional options will appear:

Local Gateway (Nexthop)
Enter the gateway or next hop address. Refer to Fig. 11.6 as an example of the responder page with the local interface set to LAN.

Remote host has fixed address
Check if the remote host has a fixed address. When enabled, incoming connections will be required to come from the defined address

Remote host
The address of the remote host from which to expect connections. This option is only available if the remote host has fixed address checkbox has been checked.

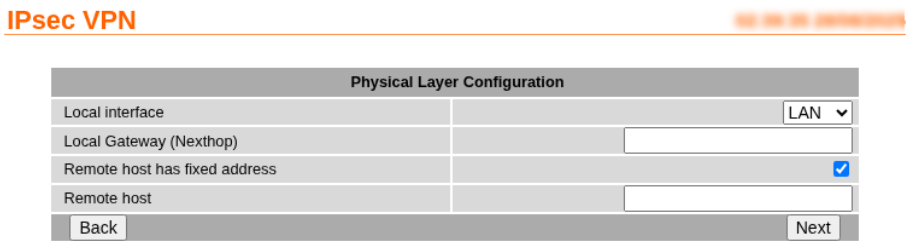


Fig. 11.6: IPsec physical configuration responder mode with LAN interface set as the

Once configuration is complete on this page click the Next button to move to the next configuration page.

Phase 1 Configuration

The Phase 1 Configuration is used to set the parameters for the first phase of IPsec Key Exchange (IKE). The first phase is a set-up phase in which the two hosts agree on how to exchange further information securely. The Phase 1 Configuration page is shown in Fig. 11.7.

The options for Phase 1 configuration are:

Authentication method
Select the authentication method from the drop-down list. The options are:

Pre-shared key
The Pre-Shared Key (PSK) is a key value which is entered into each host and is used for authentications

Certificate
A certificate is an electronic document containing a public key and a digital signature.

Enable Fragmentation
Option to allow IKE fragmentation.

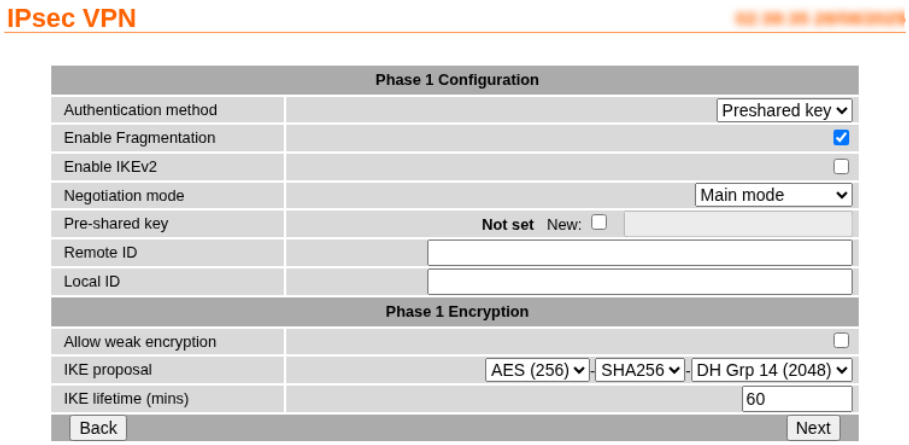


Fig. 11.7: IPsec Phase 1 configuration with Pre-Shared Key selected.

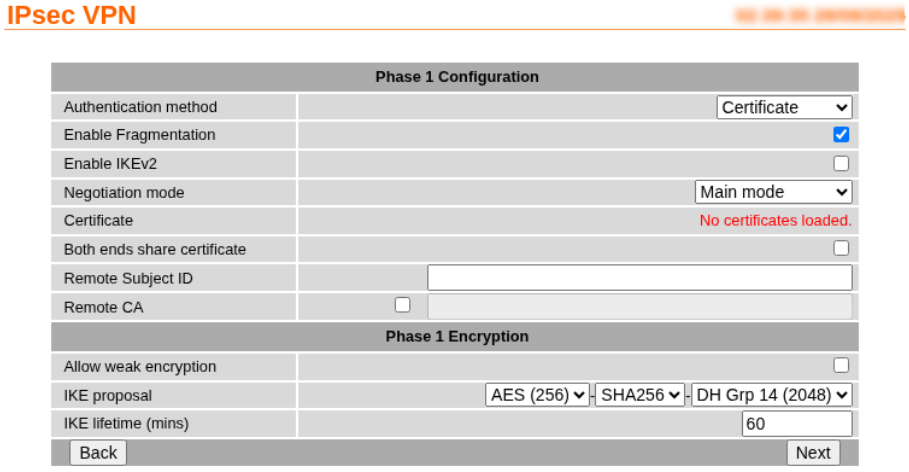


Fig. 11.8: IPsec Phase 1 configuration with certificates selected.

Enable IKEv2
Enable IKEv2 on the tunnel, as opposed to the default IKEv1. Enabling IKEv2 will remove the negotiation mode option, as it is only relevant to IKEv1.

Negotiation mode
Select the negotiated mode from the drop-down list, the options are:

Main mode
Main mode provides identity protection for the hosts initiating the session. Main mode cannot be used with pre-shared keys and name-based IDs.

Aggressive mode
Aggressive mode is quicker to establish a connection than Main mode but provides no identity protection. Aggressive mode can be used when there is Network Address Translation (NAT) on the connection between hosts.

Pre-shared key options
The following options are available when the authentication method is set to Preshared key:

Pre-shared key
This field is used to enter the Pre-Shared Key if this method of authentication was selected. To enter a new key check the box and enter the key in the text field. During key entry the key will be in clear-text, once the page is updated the key will no longer be visible. The text immediately prior the check-box will indicate if a key has been **Set** or **Not set**.

Remote ID
The remote ID is used to ensure the remote host is in fact the expected remote IPsec entity. The remote ID can take a number of forms:

IPv4
The remote party will present a standard IP address (eg 123.123.123.123) as its ID. Enter the IP address in this field.

FQDN
Fully Qualified Domain Name. The remote party will present a full hostname as its ID. Enter the name in this field. Note that hostnames must be able to be resolved through DNS.

FQUN
Fully Qualified User Name. The remote party will present a name of the form joe@some.place.com or @ipsec.server.com as its ID. The domain of this name does not have to be resolvable. Enter the name in the field, including the '@' symbol.

Distinguished Name:
Where certificate based authentication is used, the Distinguished Name or Subject string of the certificate must be entered in this field, preceded by an '@' symbol

Local ID
The local ID determines how the modem will identify itself to the remote party. The local ID can take a number of forms:

IPv4
The local ID will be a standard IP address (eg 123.123.123.123). Enter the IP address in this field.

FQDN
Fully Qualified Domain Name. The local ID will present a hostname as its ID. Enter the name in this field. Note: host-names must be able to be resolved through DNS.

FQUN
Fully Qualified User Name. The local ID is a name of the form joe@some.place.com or @ipsec.client.com. The domain of this name does not have to be resolvable. Enter the name in the field, including the '@' symbol.

Certificate options
The following options are available when the authentication method is set to Certificate:

Certificate
This config option is used to select a specific certificate, if the Certificate authentication method has been selected. For information on how to enter certificates refer to Section 11.5 Certificate Management. If no certificate is currently uploaded to the device, a message saying "No certificate loaded" will be present instead of a drop down box. If there is at least one certificate present on the device, a dropdown will be present, allowing a selection of the uploaded certificates.

Both ends share certificate
Check to indicate that both ends of the tunnel share the same certificate. If this is enabled, the certificate that is selected for the authentication, must be the same as that on the remote end of the IPsec tunnel. Enabling this removes the Remote Subject ID and Remote CA config options, as the certificate should be the same and they should therefore be known.

Remote Subject ID
The subject ID of the remote certificate. This option is only available if the certificates are not shared.

Remote CA
This is used to specify the CA that signed the certificate used by the remote end of the IPsec tunnel. This is primarily used in complex certificate setups, when the certificates used at both ends of the IPsec connection were signed by different CAs. If the same CA signed both certificates at each end of the IPsec tunnel, there should be no need to enable this config option.

The config written here should be the subject information of the CA, without a leading '@'. E.g. "C=AU, O=Test123, OU=0002, CN=Test Name"

Phase 1 Encryption

The second part of the Phase 1 configuration is the encryption type to be used. The options are:

Allow weak encryption
Check this to enable the possible selection of weak encryption options. Some encryption options are considered weak and are not recommended to be selected. This checkbox will need to be checked to select any of these options, and a warning will pop up when these options are selected.

These weak encryption options are soon to be deprecated and are currently only present for interoperability reasons. We do not recommend checking this box.

IKE proposal
IKE proposal is a set of parameters for Phase 1 IPSec negotiations. The parameters are encryption algorithms, authentication algorithm and the Diffie-Hellman group.

Encryption Algorithm
Select the encryption algorithm from the drop-down list. The options are:

AES (128)
128 bit Advanced Encryption Standard (AES).

AES (256)
256 bit Advanced Encryption Standard (AES).

3DES
Triple Data Encryption Standard (3DES).

DES
(weak) Data Encryption Standard (DES).

Authentication Algorithm
Select the authentication algorithm from the drop-down list.

The options are:

MD5
Message-Digest algorithm 5.

SHA1
Secure Hash Algorithm 1.

SHA256
Secure Hash Algorithm 2 (256 bit).

Diffie-Hellman Group
Diffie-Hellman (DH) Group is a cryptographic protocol which allows two parties to establish a shared secret key over an insecure network without the parties having any prior knowledge of the other party. Select the Diffie-Hellman Group from the drop-down list. The options are:

DH Grp 1 (768)
(weak) The 768 bit Diffie-Hellman group.

DH Grp 2 (1024)
(weak) The 1024 bit Diffie-Hellman group.

DH Grp 5 (1536)
The 1536 bit Diffie-Hellman group.

DH Grp 14 (2048)
The 2048 bit Diffie-Hellman group.

IKE lifetime (mins)
Specify the IKE lifetime in minutes. If rekeying enabled, a rekey will be attempted after the lifetime of the IKE is expired.

Once configuration is complete on this page click the Next button to move to the next configuration page.

Phase 2 Configuration

Phase 2 establishes the IPsec Security Associations (SA) parameters in order to establish an IPsec tunnel. Phase 2 has a single mode called Quick mode (called a Child SA for IKEv2) that starts after IKE has started a secure tunnel in phase 1. Quick mode is also used to re-negotiate a new IPsec SA when the current IPsec SA lifetime expires. The default Phase 2 configuration page is shown in Fig. 11.9. Fig. 11.10 shows the options available when Xauth Client is enabled. Fig. 11.11 shows the options available when Xauth Server is enabled.

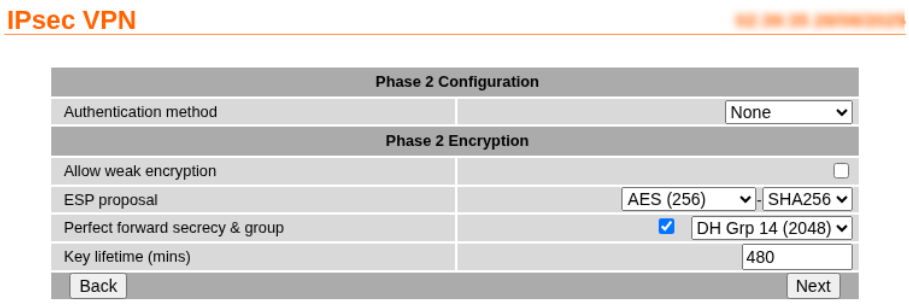


Fig. 11.9: IPsec Phase 2 configuration.

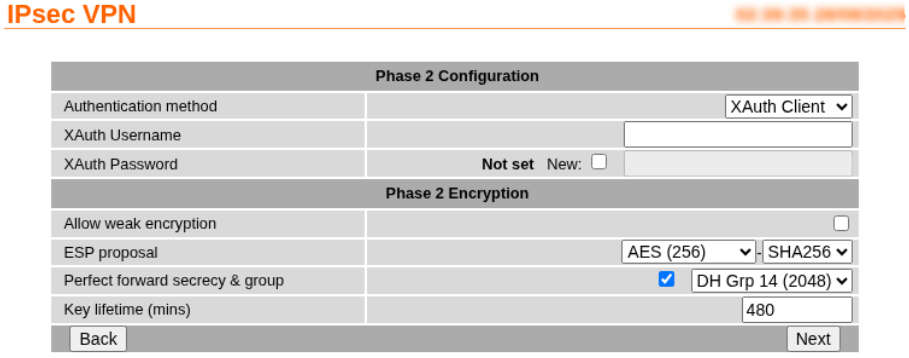


Fig. 11.10: IPsec Phase 2 configuration with Xauth Client enabled.

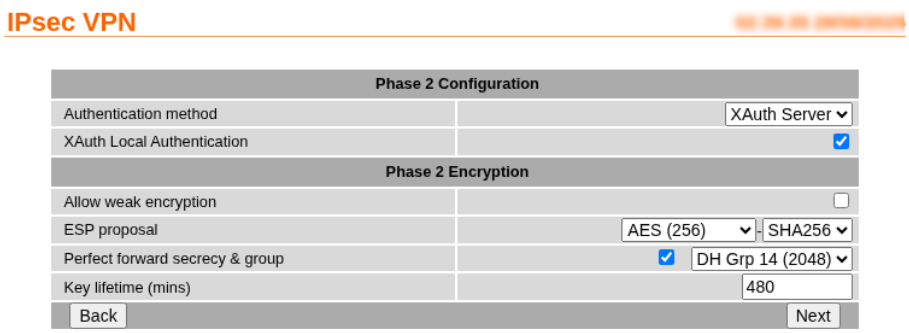


Fig. 11.11: IPsec Phase 2 configuration with Xauth Server enabled.

The phase 2 options are:

Authentication method
Select the extended authentication method, the options are:

None
No extended authentication.

XAuth Client
Provides an additional level of authentication for IKEv1. Define the user credentials for this extended authentication to allow the tunnel to authenticate properly.

XAuth username
This field is used to enter the XAuth username if this method of authentication was selected.

XAuth password
This field is used to enter the XAuth password if this method of authentication was selected. To enter a new password check the box and enter the password in the text field. During key entry the key will be in clear-text, once the page is updated the key will no longer be visible. The text immediately prior to the check-box will indicate if a key has been **Set** or **Not set**.

XAuth Server
Provides an additional level of authentication for IKEv1. Configure the authentication details for an XAuth client to authenticate against.

XAuth Local Authentication
This checkbox determines whether or not to use the authentication details/method configured for the units login. When enabled xauth will use either the standard user login method by default, or a radius server if that is configured.

When disabled a username and password field will appear that can be filled out to define credentials.

XAuth Username
This field is used to enter the XAuth username

XAuth Password
This field is used to enter the XAuth password. To enter a new password check the box and enter the password in the text field. During key entry the key will be in clear-text, once the page is updated the key will no longer be visible. The text immediately prior to the check-box will indicate if a key has been **Set** or **Not set**.

> **Note**
>
> If no username and password are defined, and local authentication is disabled, this will result in an interoperability setting that will allow any incoming xauth credentials to be accepted.

Phase 2 Encryption

The phase 2 encryption options are:

Allow weak encryption
Check this to enable the possible selection of weak encryption options. Some encryption options are considered weak and are not recommended to be selected. This checkbox will need to be checked to select any of these options, and a warning will pop up when these options are selected.

These encryption options are soon to be deprecated and are currently only present for interoperability reasons. We do not recommend checking this box.

ESP proposal
Encapsulating Security Payload (ESP) is used to encrypt the data transmitted in IP datagrams. The proposal establishes the Encryption algorithm and Authentication protocol to use.

Encryption Algorithm
Select the encryption algorithm from the drop-down list, the options are:

AES (128)
128 bit Advanced Encryption Standard (AES).

AES (256)
256 bit Advanced Encryption Standard (AES).

3DES
Triple Data Encryption Standard (3DES).

Blowfish (128)
128 bit blowfish.

Blowfish (256)
256 bit blowfish.

Twofish (128)
128 bit twofish.

Twofish (256)
256 bit twofish.

Authentication Algorithm
Select the authentication algorithm from the drop-down list, the options are:

MD5
Message-Digest algorithm 5.

SHA1
Secure Hash Algorithm 1.

SHA256
Secure Hash Algorithm 2 (256 bit).

Perfect forward secrecy & group
In an authenticated key-agreement protocol using public key cryptography, such as Diffie-Hellman key exchange, perfect forward secrecy (PFS) is the property that ensures a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

Perfect forward secrecy
Check to enable perfect forward secrecy.

Diffie-Hellman Group
Select the Diffie-Hellman Group from the drop-down list, the options are:

DH Grp 1 (768)
(weak) The 768 bit Diffie-Hellman group.

DH Grp 2 (1024)
(weak) The 1024 bit Diffie-Hellman group.

DH Grp 5 (1536)
The 1536 bit Diffie-Hellman group.

DH Grp 14 (2048)
The 2048 bit Diffie-Hellman group.

Key lifetime (mins)
Key lifetime in minutes. If rekeying is enabled, the key will be rekeyed after its lifetime has expired.

Once configuration is complete on this page click the Next button to move the next page.

Tunnel Options

Tunnel options are for configuring how the tunnel renegotiates a connection.

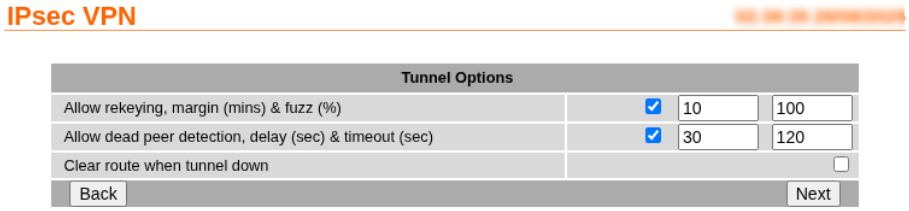


Fig. 11.12: IPsec Tunnel options and Dead Peer Detection configuration.

The options are:

Allow rekeying, margin (mins) & fuzz (%)
Re-keying is used to renegotiate the connection encryption keys prior to the previous keys expiring. The options are:

Enable
Check the check-box to enable re-keying. Default is On.

Margin
The time in minutes prior to the connection expiring at which attempts to negotiate a new connection begin. Default 10 Minutes.

Fuzz
Defines the maximum percentage by which the Margin can be increased in order to randomise re-keying intervals. Default is 100%.

Allow dead peer detection, delay & timeout
Dead Peer Detection (DPD) is a method of detecting a dead Internet Key Exchange (IKE) peer. The method uses IPsec traffic patterns to minimise the number of messages required to confirm the availability of the connection.

The configuration options are:

Enable
Check the check-box to enable Dead Peer Detection.

Delay
Set the delay in seconds between Dead Peer Detection keep-alives that are sent for the connection.

Timeout
The time in seconds to declare the peer dead after the delay and not receiving data or a keep-alive.

Clear route when tunnel down
Check to clear the routes from the routing table when the tunnel is down.

> **Warning**
>
> The clear route when tunnel down option should be used with caution.
>
> It is possible for traffic intended for a secure connection could be sent over an unsecured connection. This would occur if the routes were removed from the routing table and an alternative routing rule for example the default route allowed traffic intended for the secure tunnel to be re-directed over an insecure interface.
>
> It is recommended to leave this setting un-checked unless there is a specific requirement for it to be set.

Once configuration is complete on this page click the Next button to move the next page.

Tunnel Networks

The tunnel network page is used to configure the way in which the IPsec tunnel is terminated. The IPsec tunnel can be terminated at each end in one of two ways: host and network. In a host connection the tunnel is connected to a single IP address. In a network connection the tunnel is connected to a network subnet. The tunnel network table allows the connections for each end of the tunnel to be defined. Fig. 11.13 is an example of the Tunnel Networks page.

The options are as follows:

Enabled
Check to enable tunnel network destination. The first row/network is enabled by default. Every other one is not.

Local
Configure the local connection:

Network Host only (WAN IP)
The tunnel is connected in host mode. The IP address will be that of the wireless interface. This may not be desirable if the wireless interface is assigned a dynamic IP address as the remote end will not know the IP address and so will not be able to route traffic to it.

Host only (LAN IP)
The tunnel is connected in host mode. The IP address will be that of the LAN interface.

Host only (Looback)
The tunnel is connected in host mode. The IP address will be that of the Loopback interface. A loopback address needs to be configured on the unit for this to work properly.

Virtual Host
The tunnel is connected in host mode. The IP address will be that which is set in the address field.

LAN Subnet
The tunnel is connected in network mode to the LAN subnet.

Fig. 11.13: IPsec Tunnel networks.

Specify Subnet
The tunnel is connected in network mode to the specified subnet in the address field. A netmask must be specified in the address field for proper behaviour

All traffic
All local traffic is directed to the IPsec interface

Remote
Configure the remote connection:

Network

None
The tunnel is connected in host mode.

Specify a subnet
The tunnel is connected to the specified subnet in the address field. A netmask must be specified in the address field for proper behaviour.

All traffic
All traffic is directed to the IPsec tunnel.

Address
For host connections enter an IP address. For network connections enter a network IP address. For a network configuration of "Specify Subnet", a netmask should also be included in the address field, for example 10.10.10.0/24. The address option is only valid for "Virtual host" and "Specify Subnet".

When the configuration is complete click the Update button to add the tunnel. The main IPsec page will be displayed and the new tunnel will be added to the Tunnels table.

11.1.3 IPsec configuration example

The following example demonstrates how to add an IPsec tunnel which will connect to a remote router. Fig. 11.14 illustrates the connection which will be created in the example. The modem is configured for a standard Internet connection, this means that the IP address assigned to it will be dynamic and private. The example assumes that the router has been configured, has a static IP address and is directly accessible from the Internet. The IPsec tunnel will be terminated as a virtual host on the unit with IP address 11.22.33.44 and will be terminated on a LAN subnet at the router with address 192.168.2.0/24

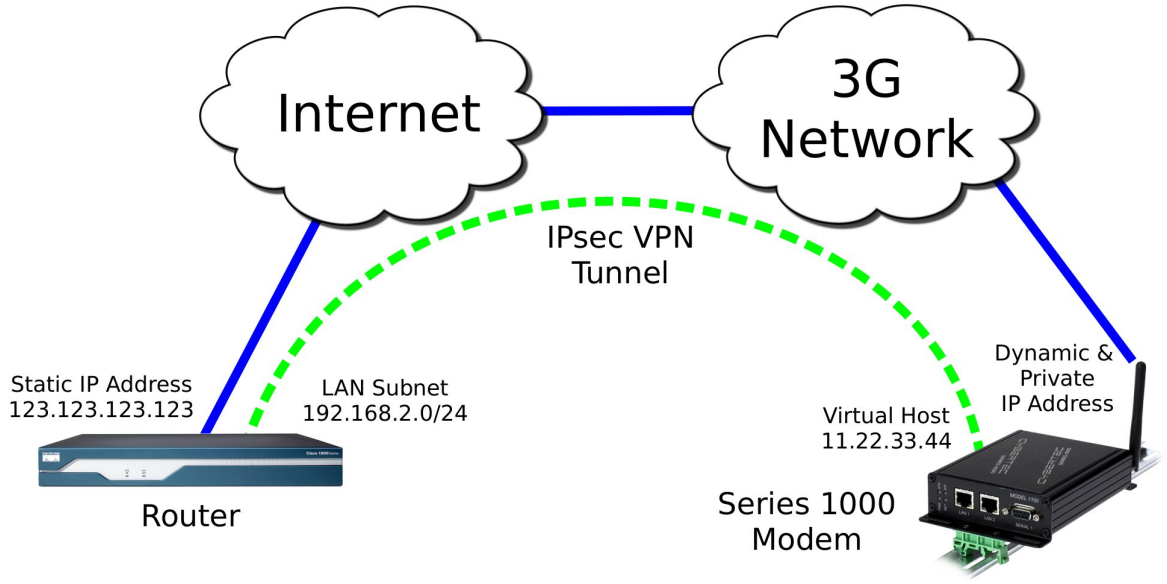


Fig. 11.14: IPsec configuration example network.

General Configuration

To start, select the IPsec main page by first clicking *VPN* → *IPsec*. Click the Add new tunnel group button. The first page of the IPsec tunnel configuration pages will be displayed, as shown in Fig. 11.15.

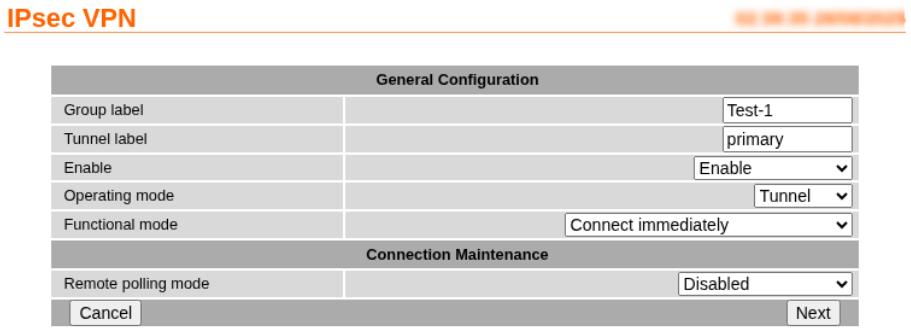


Fig. 11.15: IPsec general configuration example.

The tunnel will be named Test. It will operate in **Tunnel** mode and will act as the initiator. The configure settings required are:

General Configuration

Group label
Test-1

Tunnel label
primary

Operating mode
Tunnel

Functional mode
Connect immediately

Connection Maintenance

Remote polling mode
Disabled

Once entered click the Next button to continue to the next page.

Physical Configuration

The physical configuration page will now be displayed. Fig. 11.16 illustrates this page with the values for the example entered.

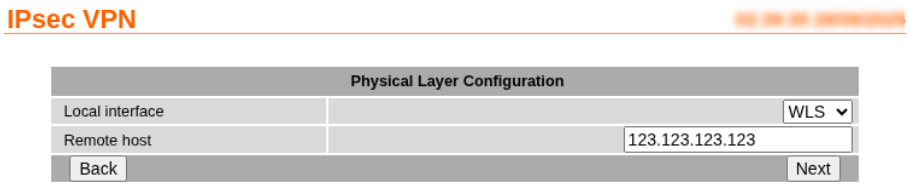


Fig. 11.16: IPsec Physical configuration example.

The tunnel is to be configured to use the wireless port and to connect to the remote host address of 123.123.123.123. The settings required are:

Physical Layer Configuration

Local interface
WLS

Remote host
123.123.123.123

Once entered click the Next button to continue to the next page.

Phase 1 Configuration

The Phase 1 Configuration page with the settings required for this example is shown in Fig. 11.17. In this phase the authentication method is set to pre-shared keys and the key entered. The remote ID is xy.example.com and local ID is ab.example.com. As the wireless IP address is dynamic and private the network provider will use Network Address Translation (NAT) so main mode cannot be used for the negotiation mode requiring the negotiating mode to be set to aggressive mode. The IKE proposal will use AES 256 bit as the encryption algorithm, SHA256 for authentication and Diffie-Hellman group 14. The IKE lifetime will be left at the default value of 60 minutes.

The required parameters are as follows:

Phase 1 Configuration

Authentication method
Pre-shared key

Negotiation mode
Aggressive mode

Pre-shared key

New
Checked

key
abcdef

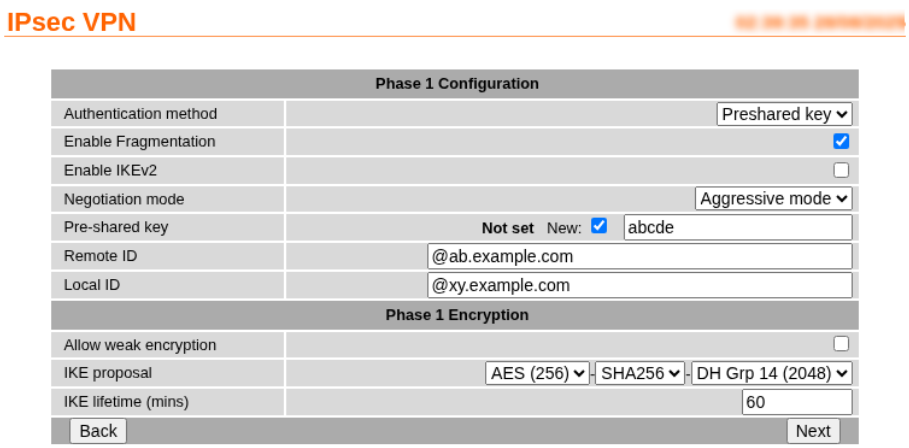


Fig. 11.17: IPsec phase 1 configuration example.

Remote ID
@ab.example.com

Local ID
@xy.example.com

Phase 1 Encryption

IKE proposal

Encryption Algorithm
AES (256)

Authentication Algorithm
SHA256

Diffie-Hellman Group
DH Grp 14 (2048)

IKE lifetime (mins)
60

Once entered click the Next button to continue to the next page.

Phase 2 Configuration

The Phase 2 Configuration page with the settings required for this example is shown in Fig. 11.18. For the Phase 2 configuration enhanced authentication will not be used, the ESP proposal encryption algorithm is set to AES 256 bit and the authentication algorithm set to SHA256. Perfect forward secrecy is enabled and set to Diffie-Hellman group 14, the key lifetime will left at the default value of 480 minutes.

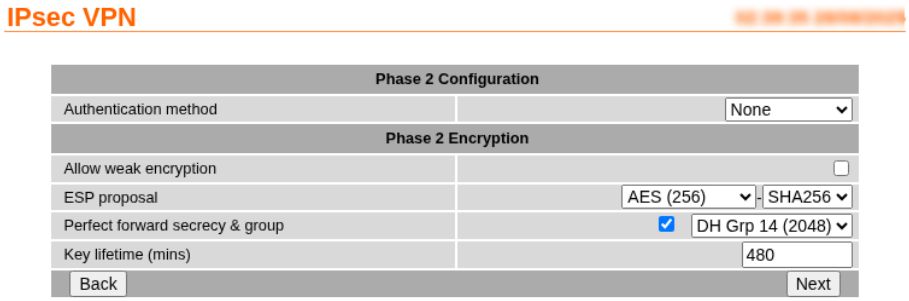


Fig. 11.18: IPsec phase 2 configuration example.

The configuration requires the following parameters to be entered:

Phase 2 Configuration

Authentication method
None

Phase 2 Encryption

ESP proposal

Encryption Algorithm
AES (256)

Authentication Algorithm
SHA256

Perfect forward secrecy & group

Perfect forward secrecy:
On (checked)

Diffie-Hellman Group
DH Grp 14 (2048)

Key lifetime (mins)
480

Once entered click the Next button to continue to the next page.

Tunnel Options & Dead Peer Detection

The Tunnels Options & Dead Peer Detection page with the settings required for this example is shown in Fig. 11.19. The re-keying options are left at the default values. Dead peer detection is enabled with the action set to clear the delay and timeout values are set to 30 and 120 seconds respectively.

The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

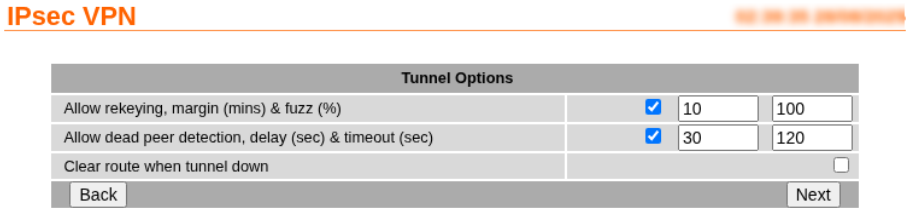


Fig. 11.19: IPsec tunnel options and Dead Peer Detection configuration example.

The configuration requires the following parameters to be entered:

Tunnel Options

Allow rekeying, margin (mins) & fuzz (%)

Enable
Checked to enable.

Margin
10 Minutes

Fuzz
100%

Allow dead peer detection, delay (sec) & timeout (sec)

Enable
Check to enable.

Delay
30

Timeout
120

Clear route when tunnel down
Un-check.

Once entered click the Next button to continue to the next page.

Tunnel Networks

The Tunnel Networks page with the settings required for this example is shown in Fig. 11.20. The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

Fig. 11.20: IPsec Tunnel Networks configuration example.

The configuration requires the following parameters to be entered:

Tunnel Networks

Enabled
Checked

Local

Network
Virtual Host

Address
11.22.33.44

Remote

Network
Specify a subnet

Address
192.168.2.0/24

To complete the process of adding the tunnel click the Update button. The tunnel will be saved and the General IPsec Configuration page will again be displayed, now with the new tunnel added to the Tunnels table, as shown in Fig. 11.21.

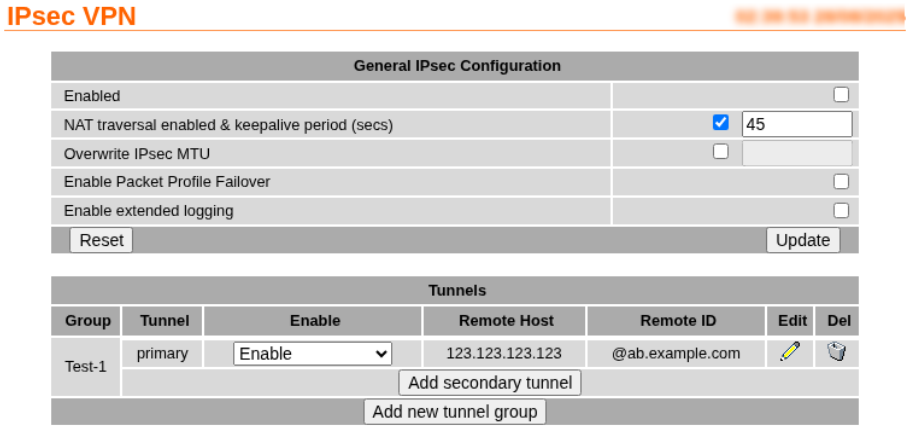


Fig. 11.21: IPsec table with the newly created entry.

Enable Tunnel

Once a tunnel is configured, user can change whether it is enabled by using the drop down that is present in the Enable column.

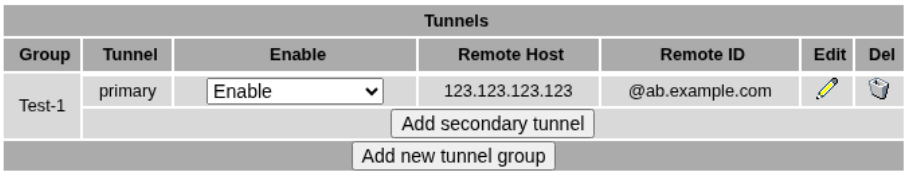


Fig. 11.22: IPsec tunnels with the Enable drop down.

Select whether the tunnel should be allowed to start. The options are:

Disable
Don't start up this tunnel

Enable
Start up the tunnel. Note that if this tunnel is configured to use the WAN interface in any way, that this tunnel will not start up until the WAN interface has been successfully brought up.

Enable On VRRP
Start up the tunnel when the unit becomes a VRRP master. This requires VRRP to be running on the device to work properly.

Making a change to a drop down of an IPsec tunnel will immediately commit and save the change.

Enable IPsec

To complete the configuration in the General IPsec Configuration enable IPsec by checking the **Enabled** check-box and enable **NAT traversal**. The page for this configuration is shown in Fig. 11.23.

Click the Update button to save the settings.

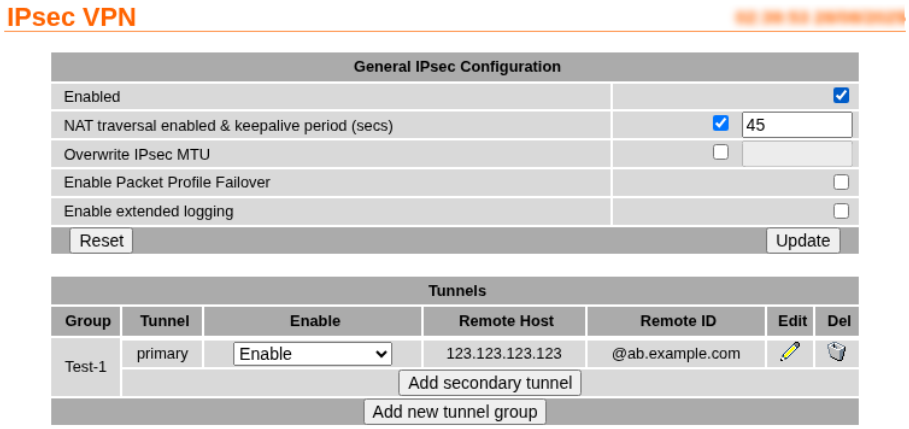


Fig. 11.23: IPsec based VPN main page, with IPsec enabled.

IPsec Status

Once the settings have been saved IPsec will start and attempt to establish a tunnel with the remote host. Note that this may take several minutes to complete. To check the status of the tunnel click *Status* → *VPN*. A page similar to that shown in Fig. 11.24 will be displayed. If the status of the tunnel is **Connected** then the tunnel has been established and data can be passed over it.

If no tunnels are currently running then the status page will just say "No VPNs enabled".

To obtain further details on the VPN connection click the link **Detailed IPsec status**. A page similar to that shown in Fig. 11.25 will be displayed. This information is usually only required if the link is not behaving as expected or if the tunnel is not able to be established.

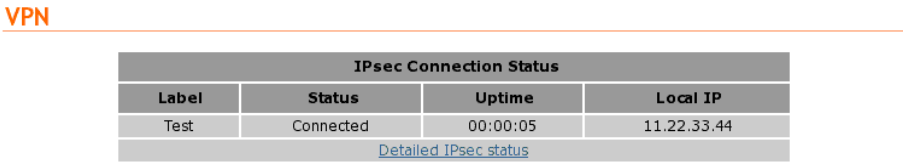


Fig. 11.24: IPsec connection status.

Note

The status web pages do not automatically refresh so it may be necessary to refresh the page to obtain the current status.

Note

When the detailed page is selected or refreshed it will automatically scroll to the last entry in the log.

To view earlier entries the right hand scroll bar can be used.

11.1.4 Adding a Secondary Tunnel

A secondary tunnel can be added once a tunnel group and primary tunnel have been defined. The secondary tunnel will be used when the primary connection cannot be established.

To add a secondary tunnel click the Add secondary tunnel button within the tunnel group in which the tunnel is to be added. A page similar to that shown in Fig. 11.26 will be displayed.

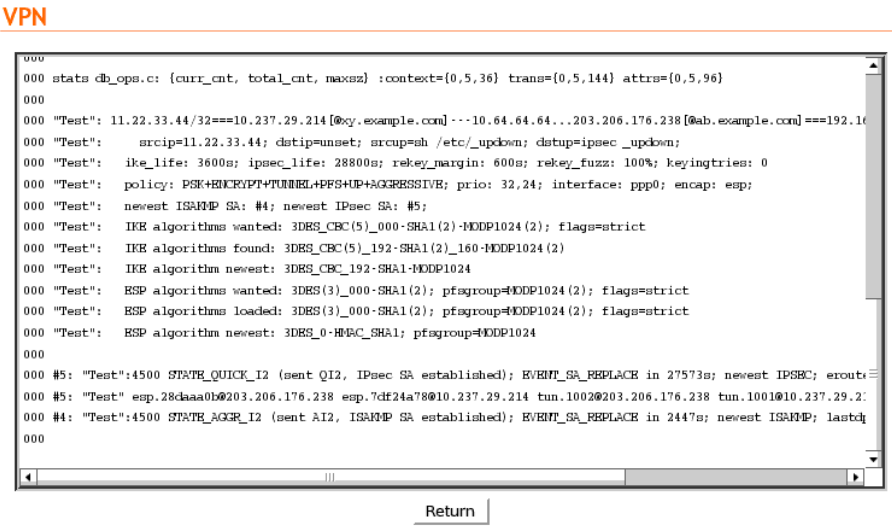


Fig. 11.25: IPsec connection status details.

Note

Each configured tunnel group includes an Add secondary tunnel button. Click this button within the desired group to add a secondary tunnel to that group.

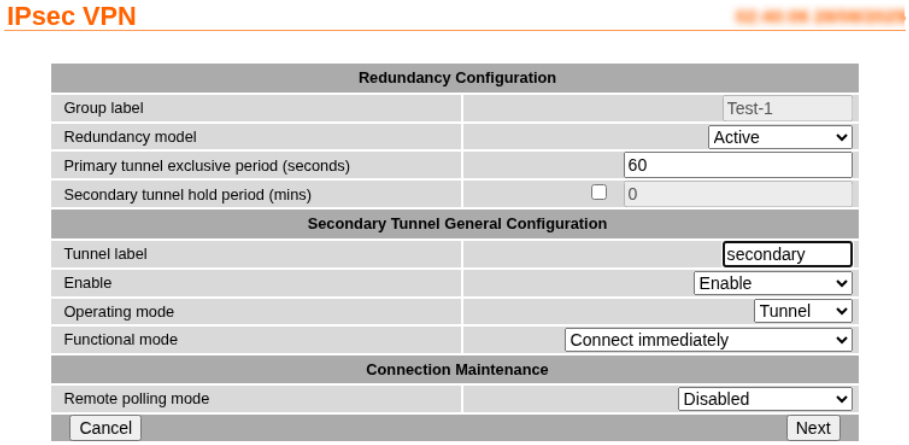


Fig. 11.26: Adding a secondary IPsec tunnel.

The options vary between redundancy operating modes. The passive redundancy modes are **Rotate** and **Try Primary First**, while the active redundancy mode is **Active**. The active redundancy options are shown in Fig. 11.26 and the passive options are shown in Fig. 11.27.

Redundancy Configuration

Group label

The group label for the tunnel group. This will match the tunnel group for which the Add secondary tunnel button was pressed. This will be non configurable for a secondary tunnel, as the group label can not be changed once set and it was set when creating the primary tunnel.

Redundancy model

Set the redundancy model to use for the tunnel group from the dropdown which contains three options. **Rotate** and **Try Primary First** are passive redundancy modes, while **Active** is active redundancy

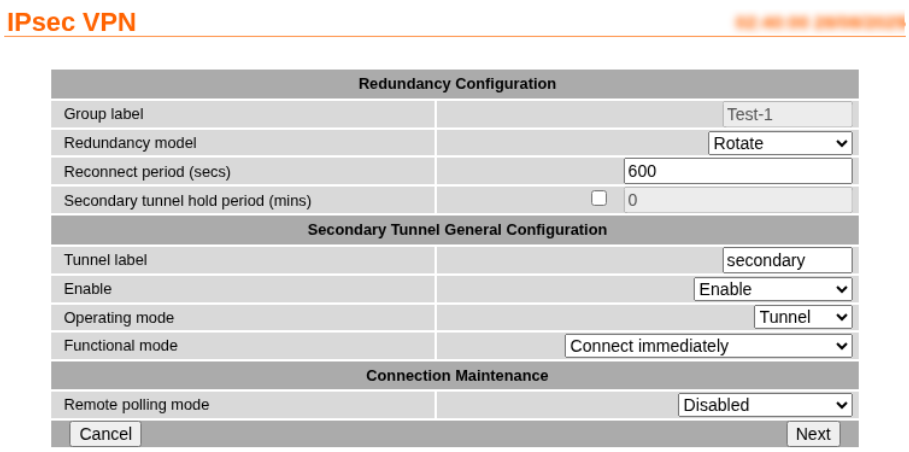


Fig. 11.27: Adding a backup IPsec tunnel.

mode. Depending on whether an active or passive type of redundancy model is chosen, will determine other config options. The options are:

Rotate (passive redundancy)
When either primary or secondary connections fail the other will be tried until a connection is established.

Try primary first (passive redundancy)
When either primary or secondary tunnels fail try the primary first then the secondary until a connection is established.

Active (active redundancy)
If the secondary tunnel has a connection established attempt to establish the primary connection in the background. If the connection to the primary is then established switch to the primary and disconnect the secondary.

Reconnect period (passive redundancy)
Time to wait from a connection failure to attempting to establish a connection on the other tunnel.

Primary tunnel exclusive period (active redundancy)
The time after start-up for which the primary tunnel only will attempt to establish a connection. Once this time has expired if the primary has not connected to secondary will also be tried.

Secondary tunnel hold period

Enable
Check to enable

Period

Passive redundancy
The time before disconnecting the backup tunnel and going back to the primary tunnel.

Active redundancy
The time before the primary tunnel attempts to reconnect.

Secondary Tunnel General Configuration
IPsec general configuration for the backup IPsec tunnel. The options are as follows:

Tunnel label
Set the label or name for the tunnel within the group. This is used to distinguish between tunnels for example 'primary' and 'secondary'

Enable
Check to enable.

Operating mode
Select the operating mode of the IPsec tunnel from the following options:

Tunnel
Tunnel mode encapsulates the entire IP packet to provide a secure connection between two gateways. In tunnel mode the payload, the header and the routing information are all encrypted, and then encapsulated into a new IP packet. This mode is generally used to create a VPN.

Transport
Transport mode provides a secure connection between two hosts. Only the payload of the IP packet is encrypted.

Functional mode
Select the functional mode of the IPsec tunnel from the following options:

Connect immediately
The tunnel will be initiated, that is it will attempt to establish a connection with a remote responder.

Responder or Connect on demand
Wait for and respond to incoming connections or if no active connection, establish a connection to a remote server.

Connection Maintenance
IPsec connection maintenance options:

Remote polling mode

Disabled
No remote polling.

Poll at fixed interval
Enable polling that will occur at a regular interval, until no responses are received. More configuration options will appear when this mode is selected. The options are:

Poll period (secs, min 15)
Specify the time interval, in seconds, between polls. Minimum value of 15 seconds.

Retry period (secs, min 15, max poll period)
Check to enable and specify the time, in seconds, to retry the poll after a failed poll has occurred. Minimum value is 15 seconds. Max value is the value configured for the poll period.

Failed establishment polls before restarting the connection
Specify the number of failed establishment polls to declare the connection down and restart the establishment process. Polling will only occur on the establishment of the connection to ensure it is running as intended.

Failed polls before restarting the connection
Specify the number of failed polls to declare the connection down and to restart the establishment process. This value must be 1 or greater.

Poll Type
Specify the poll type to use. The options are:

Ping (ICMP)
Use pings to poll the specified address

TCP Socket
Establish a TCP socket to the specified address and port number. The TCP connection will be terminated as soon as it is successfully opened.

Source address
Check to enable a source address. Source address configures a source address to be used when polling remote the address. The configured source address must be a valid address for the poll to use, not just a valid ip address, but the source address must make sense for the interface. This is not normally needed, and is normally used when there are multiple potential source addresses for the remote poller to use, which is dependent on the tunnel mappings configured.

Poll address
Specify the remote IP address to poll. It is recommended for this to be something that can only be accessed once the tunnel is up. If the poll type is TCP Socket the port number should also be included in this field. It should be in the format <IP>:<port>

Once configuration is complete on this page click the Next button to move to the next page.

The remaining options are the same as when configuring a primary tunnel. The next page will be the Physical Layer Configuration to continue the configuration go to the *Physical Configuration* Section and continue through the configuration pages.

11.1.5 Example of Adding a Backup IPsec Tunnel

The following example demonstrates how to add a backup IPsec tunnel to the configuration described in IPsec configuration example. The backup IPsec tunnel will be terminated as a virtual host on the unit with IP address 11.22.33.44 and will be terminated on a LAN subnet at the router with address 192.168.2.0/24

General Configuration

To start, select the IPsec main page by first clicking *VPN* → *IPsecVPN* then click the Add backup tunnel button within the group Test-1 in the tunnels table. The first page of the IPsec tunnel configuration pages will be displayed, as shown in Fig. 11.28.

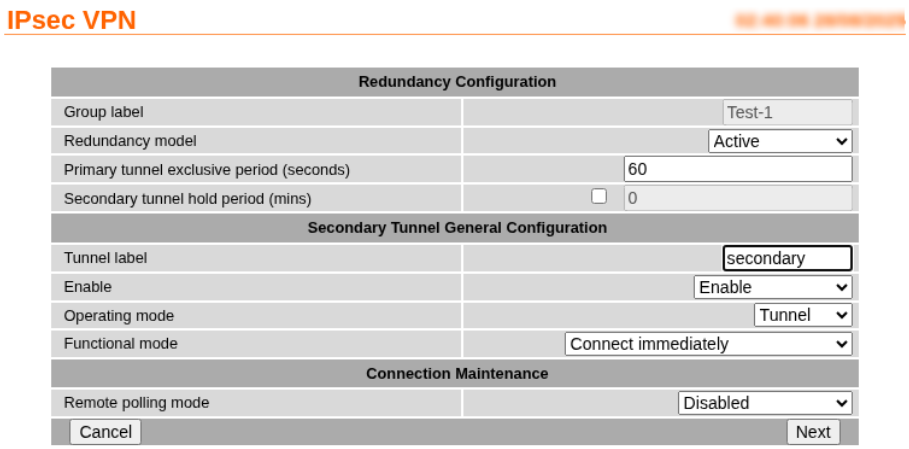


Fig. 11.28: Backup IPsec tunnel configuration example.

The configuration is such that the Primary tunnel should be use whenever possible, so the redundancy model will be active with the secondary hold time disabled. The backup tunnel is to be called secondary, it will operate in **Tunnel** mode and will act as the initiator. The configure settings required are:

Redundancy Configuration

Group label
Test-1

Redundancy model
Active

Primary tunnel exclusive period
60

Secondary tunnel hold time
Disabled

Secondary Tunnel General Configuration

Tunnel label
secondary

Operating mode
Tunnel

Functional mode
Connect immediately

Connection Maintenance

Remote polling mode
Disabled

Once entered click the Next button to continue to the next page.

Physical Configuration

The physical configuration page will now be displayed. Fig. 11.29 illustrates this page with the values for the example entered.

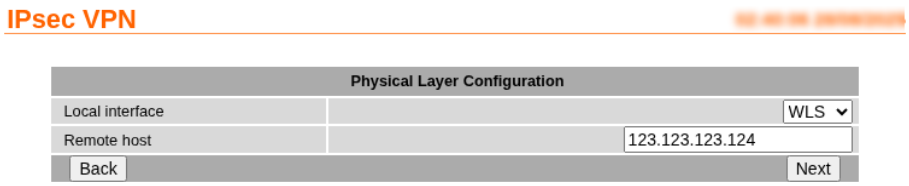


Fig. 11.29: IPsec Physical configuration example.

The tunnel is to be configured to use the wireless port and to connect to the remote host address of 123.123.123.124. The settings required are:

Physical Layer Configuration

Local interface
WLS

Remote host
123.123.123.124

Once entered click the Next button to continue to the next page.

Phase 1 Configuration

The Phase 1 Configuration page with the settings required for this example is shown in Fig. 11.30. In this phase the authentication method is set to pre-shared keys and the key entered. The remote ID is xy.example.com and local ID is ab.example.com. As the wireless IP address is dynamic and private the network provider will use Network Address Translation (NAT) so main mode cannot be used for the negotiation mode requiring the negotiating mode to be set to aggressive mode. The IKE proposal will use AES 256 bit as the encryption algorithm, SHA256 for authentication and Diffie-Hellman group 14. The IKE lifetime will be left at the default value of 60 minutes.

The required parameters are as follows:

Phase 1 Configuration

Authentication method
Pre-shared key

Negotiation mode
Aggressive mode

Pre-shared key

New
Checked

key
abcdef

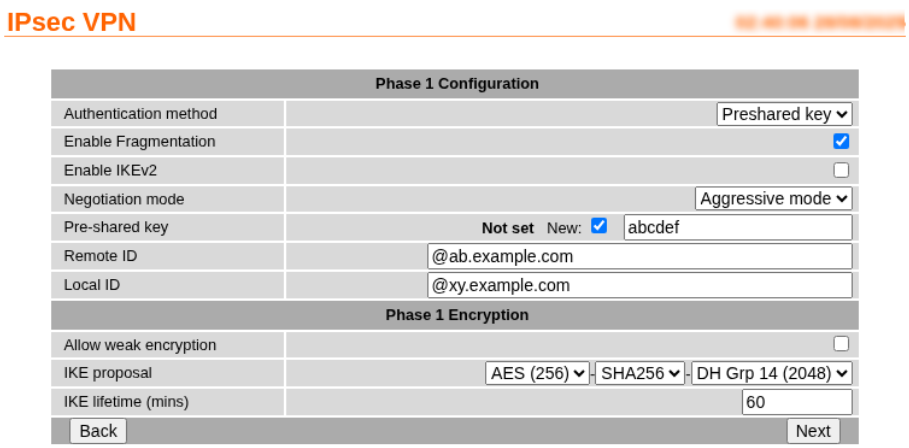


Fig. 11.30: IPsec phase 1 configuration example.

Remote ID
@ab.example.com

Local ID
@xy.example.com

Phase 1 Encryption

IKE proposal

Encryption Algorithm
AES (256)

Authentication Algorithm
SHA256

Diffie-Hellman Group
DH Grp 14 (2048)

IKE lifetime (mins)
60

Once entered click the Next button to continue to the next page.

Phase 2 Configuration

The Phase 2 Configuration page with the settings required for this example is shown in Fig. 11.31. For the Phase 2 configuration enhanced authentication will not be used, the ESP proposal encryption algorithm is set to AES 256 bit and the authentication algorithm set to SHA256. Perfect forward secrecy is enabled and set to Diffie-Hellman group 14, the key lifetime will left at the default value of 480 minutes.

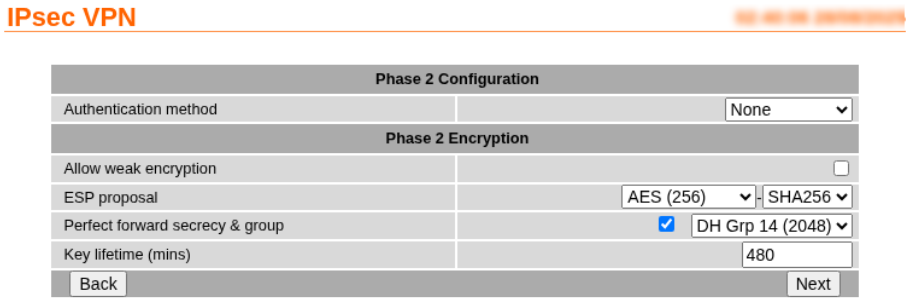


Fig. 11.31: IPsec phase 2 configuration example.

The configuration requires the following parameters to be entered:

Phase 2 Configuration

Authentication method
None

Phase 2 Encryption

ESP proposal

Encryption Algorithm
AES (256)

Authentication Algorithm
SHA256

Perfect forward secrecy & group

Perfect forward secrecy
On (checked)

Diffie-Hellman Group
DH Grp 14 (2048)

Key lifetime (mins)
480

Once entered click the Next button to continue to the next page.

Tunnel Options & Dead Peer Detection

The Tunnels Options & Dead Peer Detection page with the settings required for this example is shown in Fig. 11.32. The re-keying options are left at the default values. Dead peer detection is enabled with the action set to clear the delay and timeout values are set to 30 and 120 seconds respectively.

The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

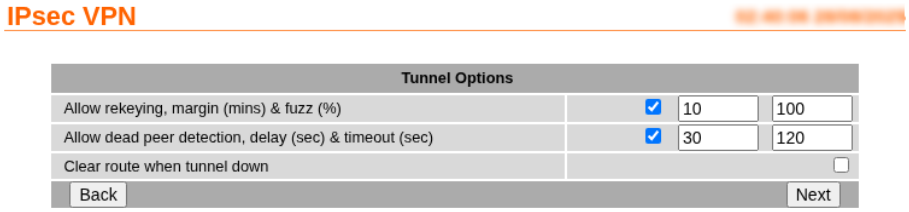


Fig. 11.32: IPsec tunnel options and Dead Peer Detection configuration example.

The configuration requires the following parameters to be entered:

Tunnel Options

Allow rekeying, margin (mins) & fuzz (%)

Enable
Check to enable.

Margin
10 Minutes

Fuzz
100%

Allow dead peer detection, delay (sec) & timeout (sec)

Enable
Check to enable.

Delay
30

Timeout
120

Clear route when tunnel down

Enable
Un-check.

Once entered click the Next button to continue to the next page.

Tunnel Networks

The Tunnel Networks page with the settings required for this example is shown in Fig. 11.33. The local tunnel will be configured as a virtual host with the IP address 11.22.33.44 and the remote connection will be to the LAN 192.168.2.0/24.

Fig. 11.33: IPsec Tunnel Networks configuration example.

The configuration requires the following parameters to be entered:

Tunnel Networks

Enabled
Checked

Local

Network
Virtual Host

Address
11.22.33.44

Remote

Network
Specify a subnet

Address
192.168.2.0/24

To complete the process of adding the tunnel click the Update button. The tunnel will be saved and the General IPsec Configuration page will again be displayed, now with the backup tunnel added to the tunnel group in the Tunnels table, as shown in Fig. 11.34.

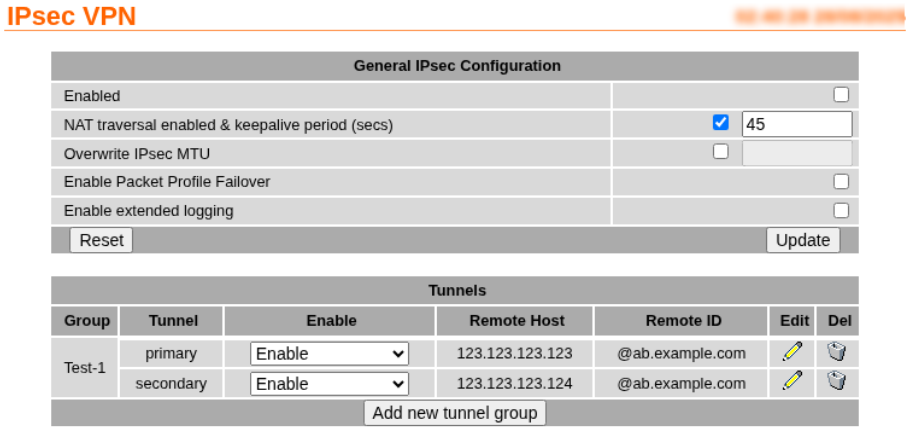


Fig. 11.34: IPsec table with the newly created entry.

11.1.6 Editing an IPsec Tunnel

To edit an IPsec tunnel click the icon in the Edit column in the row of the tunnel to be edited inside the Tunnels table. The process of editing is similar to that of adding a tunnel described in Adding an IPsec tunnel. The group label will not be configurable and will be grayed out.

11.1.7 Deleting an IPsec Tunnel

To delete an IPsec tunnel click the icon in the Del column in the row of the tunnel to be deleted inside the Tunnels table. A confirmation pop up will appear asking if you want to delete the tunnel. Deleting a primary tunnel will delete the whole group. Deleting a secondary tunnel will just delete the secondary tunnel.

11.1.8 Example of Deleting an IPsec Tunnel

To delete the backup tunnel created in the previous example click the icon in the Del column of the tunnel called secondary in the group Test-1. A pop-up box will be displayed requesting confirmation, as shown in Fig. 11.35.

Click the OK button to confirm the deletion. The page will update and the secondary tunnel will be removed from the Tunnels table, as shown in Fig. 11.36.

11.1.9 Door Knock

Adding a door knock

A door knock will attempt to make an HTTPS GET request to the specified address, and include the specified parameters in that request. If an existing IPsec group and tunnel is specified for the door knock, said specified tunnel will attempt to start up. This is not a requirement when creating a door knock.

Door knocks are an implementation of port knocking and can be used to trigger firewall rule changes on external devices.

The door knock will occur on configuration change and/or enabling of the door knock. This will occur regardless of the configured resend period.

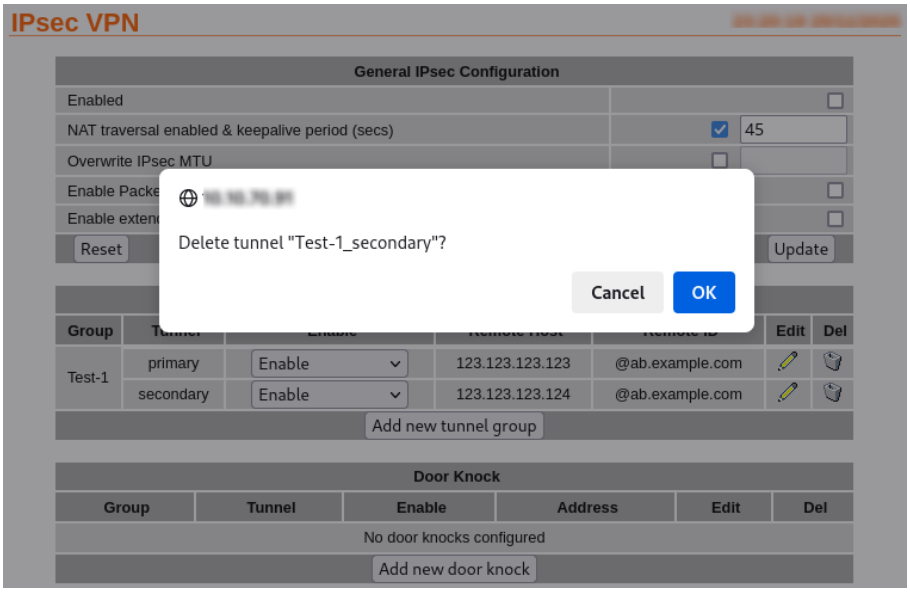


Fig. 11.35: Deleting the backup IPsec tunnel 'secondary'.

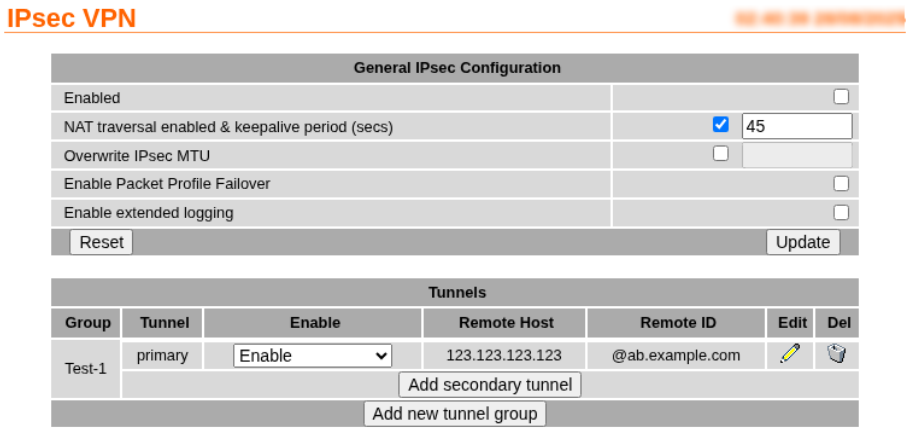


Fig. 11.36: IPsec tunnels table after deleting the 'secondary' tunnel.

To add a door knock, click Add new door knock in the **Door Knock** table on the *VPN → IPsec* page.

The configuration page for the new door knock will appear, as shown in Fig. 11.37.

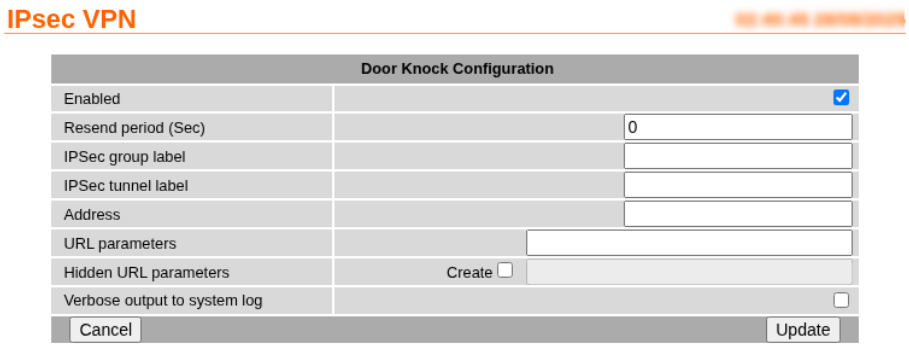


Fig. 11.37: Adding a door knock.

The options are as follows:

Enabled
Check the checkbox to enable the door knock

Resend period (Sec)
Indicates the frequency with which to perform the door knock. A value of 0 will not attempt to retry the door knock.

IPSec group label
The group label of the IPsec tunnel to attempt to start. A valid group and tunnel that match an existing tunnel are required for this to start the tunnel. It is not required to start a tunnel as part of the door knock

IPSec tunnel label
The tunnel label of the IPsec tunnel to attempt to start. A valid group and tunnel that match an existing tunnel are required for this to start the tunnel. It is not required to start a tunnel as part of the door knock

Address
Address for the url

URL parameters
URL parameters to include after the address. If there are multiple parameters, these should be separated by an '&', as is done in a URL. These URL parameters will automatically be prepended with a '/' so that is not required.

Hidden URL parameters
Hidden URL parameters to include after the address. To configure these parameters, check the checkbox to the left of the textfield. If there are multiple parameters, these should be separated by an '&', as is done in a URL. These Hidden URL parameters will automatically be prepended with a '/' if there were no non Hidden URL parameters. If there were non Hidden URL parameters, these Hidden URL parameters will be prepended with an & automatically.

If there are no previously configured parameters, it will say "Create" to the immediate left of the checkbox. If there are previously configured parameters, it will say "Exists" in bold and the "Change" to the immediate left of the checkbox.

Verbose output to system log
When enabled, output door knock attempts to the syslog. Hidden URL parameters are hidden from the output.

An example of a door knock configuration is shown in Fig. 11.38.

To commit and save the configuration, click Update. The configured door knock should now appear in the door knock table of the main IPsec VPN page.

An example of what the table will look like with a configured door knock is shown in Fig. 11.39.

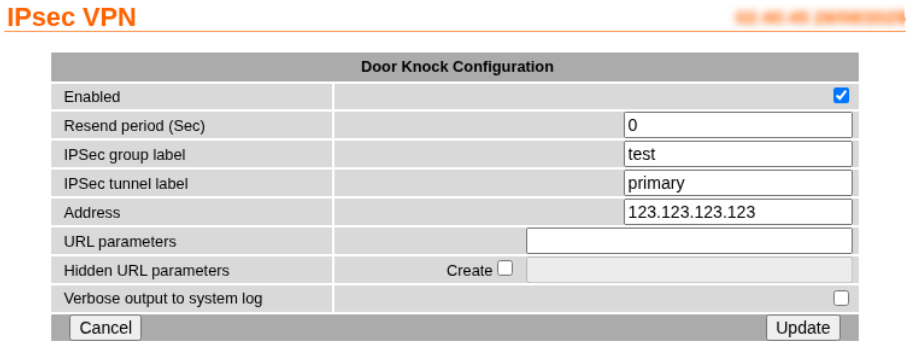


Fig. 11.38: Example of a door knock configuration.

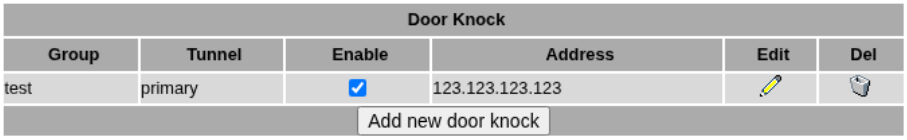


Fig. 11.39: Example of a configured door knock.

The door knock can be disabled/enabled by checking the checkbox in the Enable column of the Door Knock table. Doing so will immediately commit and save the change.

Editing a Door Knock

To edit a door knock click the  icon in the Edit column in the row of the door knock to be edited, inside the door knock table. The process of editing is similar to that of adding a door knock described in Adding a door knock.

Deleting a Door Knock

To delete a door knock, click the  icon in the Del column in the row of the door knock to be deleted, inside the door knock table. A confirmation pop up will appear asking if you want to delete the door knock.

11.2 Secure Sockets Layer (SSL) VPN

Secure Sockets Layer (SSL) are cryptographic protocols that provide secure communications over a communications network. SSL operates at the transport layer (layer 4 of the OSI model). This means that it is can be used to create a tunnel through which other layer 4 protocols such as TCP and UDP can pass.

The SSL VPN implementation in the modem is OpenVPN. OpenVPN which is a free and open source virtual private network (VPN) program for creating point-to-point or server-to-multiclient encrypted tunnels. It is capable of establishing direct links between computers that are behind NAT firewalls. For information on installing and configuring OpenVPN refer to the OpenVPN website.

11.2.1 SSL VPN configuration

To access the SSL VPN configuration page, select *VPN* → *SSL*. A page similar to that shown in Fig. 11.40 will be displayed.

The configuration options are divided into **Basic Configuration** in the upper section of the page and optional **Advanced Configuration** in the lower section of the page.

Basic Configuration

The Basic Configurations options are as follows:

Enabled

Check the box to enable the SSL VPN.

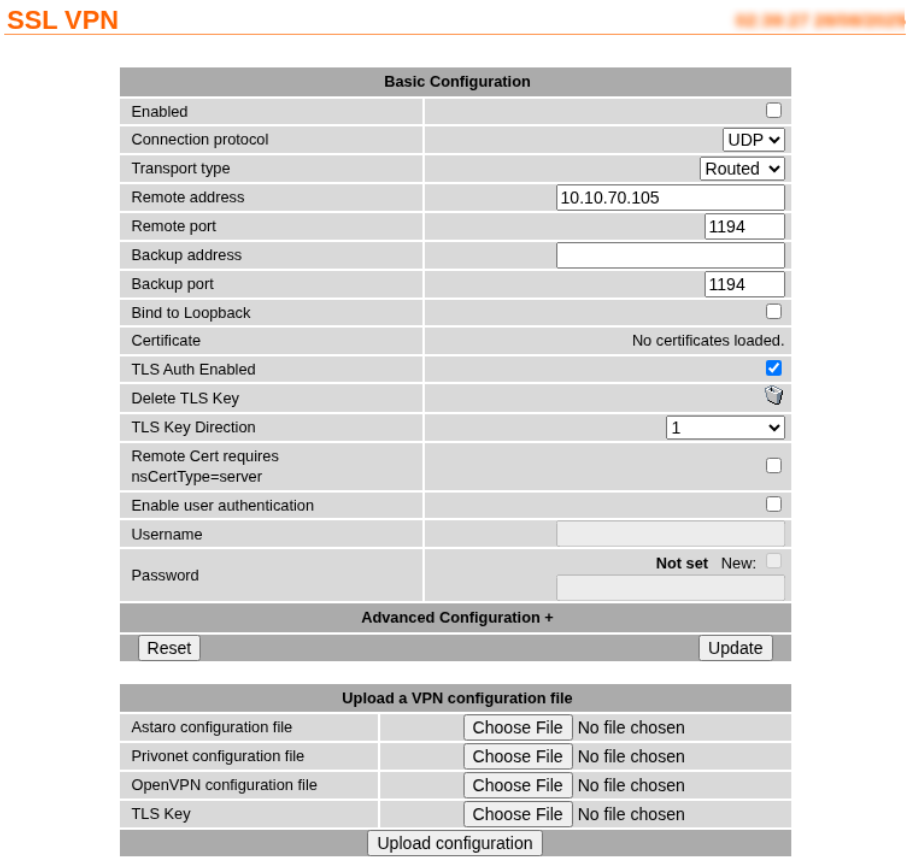


Fig. 11.40: SSL based VPN configuration web page.

Connection Protocol
The protocol used will be must match the configuration of the remote VPN server this tunnel will be established to. Select UDP or TCP as appropriate. Default is UDP.

Transport Type
Select the transport type. The transport used must match the configuration of the remote VPN server.

Bridged
Bridging is a technique for creating a virtual, wide-area Ethernet LAN, running on a single subnet. The advantages of bridging are broadcasts will transverse the VPN which in same situations is desirable, and no routing rules are required. The disadvantages are broadcasts can be problematic on a wireless network as the over-the-air traffic is increased and bridging does not scale well as new devices are added to the network.

Routed
Routing will create a separate subnet for each VPN connection. To access one subnet from another requires routing rules to be configured at the VPN router. The advantages of routing are efficiency, scalability and no broadcast traffic. This is particularly important with wireless networks to reduce the over-the-air traffic. The disadvantage is that routing rules are required which adds to the configuration.

Remote address
Specify the address of the remote VPN server.

Remote port
Specify the port number of the remote VPN server. The default OpenVPN port number is 1194.

Bind to Loopback
Check to bind the service to the loopback port. Refer to the *Loopback Interface* section for details on configuring the loopback interface.

Certificate
Specify the certificate to use for authentication. For details on how to load certificates refer to *Certificate Management*.

TLS Auth Enabled
Check to enable TLS authentication.

TLS Key Direction
Specify the direction of the TLS key. The options are:

bidirectional
The key is used for both incoming and outgoing packets.

0
The key is used for incoming packets only.

1
The key is used for outgoing packets only.

Remote Cert requires nsCertType=server
The server certificate may have the ns Cert Type set to server. If this is the case this Check to enable this parameter.

Enable user authentication
Check to enable user authentication

Username
The user name to use for authentication.

Password
The password to use for authentication.

Click the Update button to save and commit changes.

Advanced Configuration
The advanced options provide more control of the VPN. For most applications the default options do not

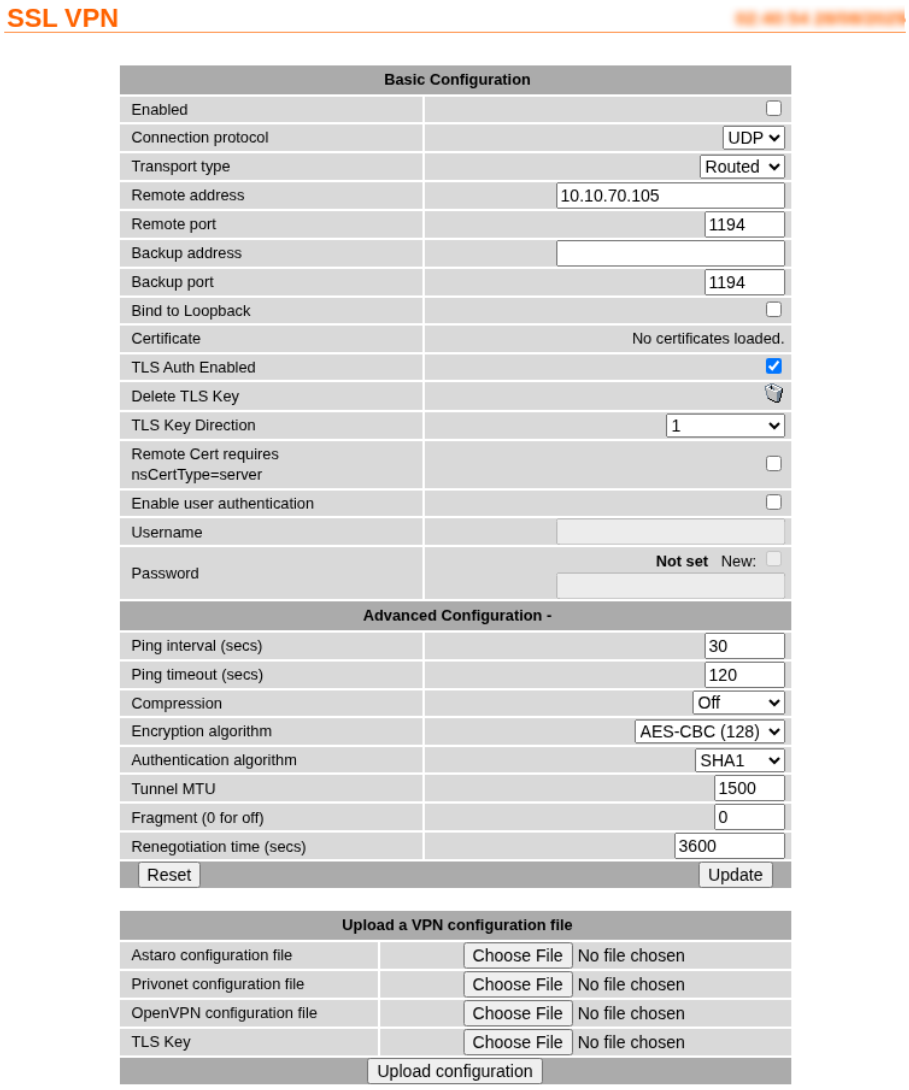


Fig. 11.41: SSL based VPN configuration web page showing advanced options.

need to be changed. To access the advanced configuration options click the Advanced Configuration title, the advanced options will then drop down as shown in Fig. 11.41. The Advanced Configurations options are as follows:

Ping interval (secs)
Specify the interval in seconds at which to ping the remote server. This is used to determine the status of the connection.

Ping timeout (secs)
Specify the ping time-out in seconds. This is used to determine if the VPN connection has terminated. If this time is exceeded without receiving a ping response from the server the connection will be re-established.

Compression
Specify if compression is to be used for the data being transmitted through the VPN tunnel. This must match the compression setting at the remote VPN server. Select one of the following options from the drop-down list:

Off
Compression is disabled.

Adaptive
The performance will be measured with compression on and with compression off, the option with the higher performance will be selected.

On
Compression is enabled.

Encryption algorithm
Specify the encryption algorithm to use from the drop-down list. The options are:

DES (64)
Data Encryption Standard.

3DES (192)
192 bit Triple Data Encryption Standard.

Blowfish (128)
128 bit Blowfish.

AES-CBC (128)
128 bit Advanced Encryption Standard in Cipher Block Chaining mode (AES-CBC).

AES-CBC (192)
192 bit Advanced Encryption Standard in Cipher Block Chaining mode (AES-CBC).

AES-CBC (256)
256 bit Advanced Encryption Standard in Cipher Block Chaining mode (AES-CBC).

AES-GCM (128)
128 bit Advanced Encryption Standard in Galois/Counter mode (AES-GCM).

AES-GCM (192)
192 bit Advanced Encryption Standard in Galois/Counter mode (AES-GCM).

AES-GCM (256)
256 bit Advanced Encryption Standard in Galois/Counter mode (AES-GCM).

Tunnel MTU
Specify the MTU of the tunnel.

Fragment (0 for off)
Used for UDP only. Meant as a last resort when MTU path discovery does not work.

Renegotiation time (secs)
The time at which the data channel key will be renegotiated.

Click the Update button to save and commit changes.

Upload a VPN configuration file
VPN Configuration files of the following types may be uploaded to the unit:

Astaro configuration file
A configuration file generated by an Astaro Security Gateway Appliance.

Privonet configuration file
A configuration file for the Privonet service. Privonet

Click the Choose file button to select the configuration file, then click the Upload configuration button to upload the configuration file to the unit.

11.2.2 Connecting to a VPN server

This section describes an example of connecting to a VPN server. Fig. 11.42 illustrates the network which will be established. For this example a connection will be established from the unit to an OpenVPN server using a routed connection and UDP as the connection protocol. The IP address of the OpenVPN server is 123.123.123.123 and the port number is 1194. The certificate supplied for authentication is called demoClient. To ensure the connection remains connected the ping interval will be set to 30 seconds with a time-out of 120 seconds. Compression will be disabled and the Encryption algorithm will be 128 bit Blowfish.

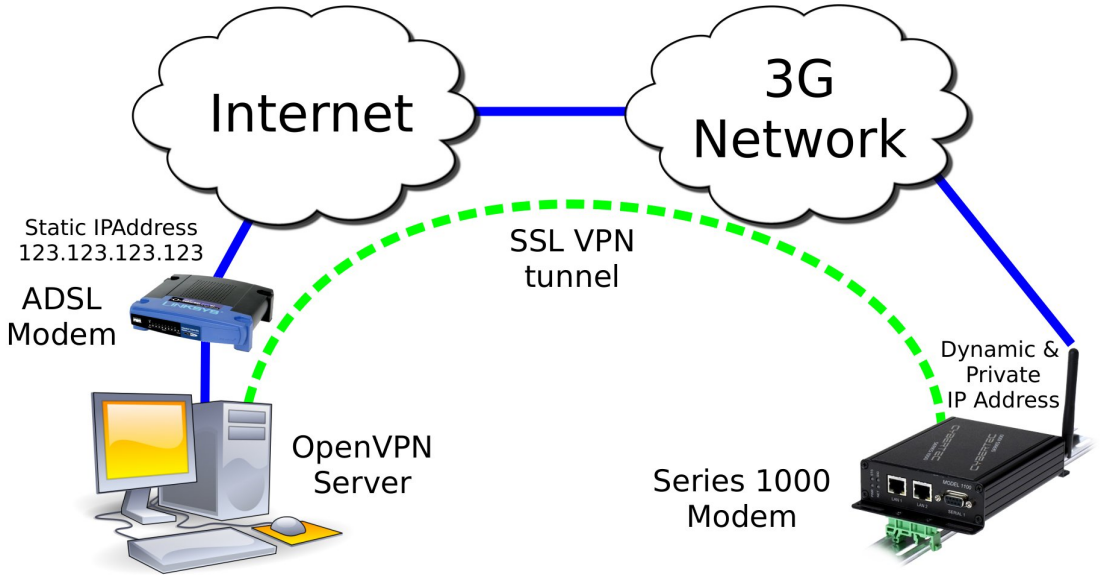


Fig. 11.42: SSL based VPN example network.

Select **VPN** on the main menu to display the the SSL VPN configuration page. Fig. 11.43 shows the SSL VPN configuration page with the options set for the example.

The following are configuration settings used for the example:

Basic Configuration

Enabled
Checked

Connection Protocol
UDP

Transport Type
Routed

Remote address
123.123.123.123

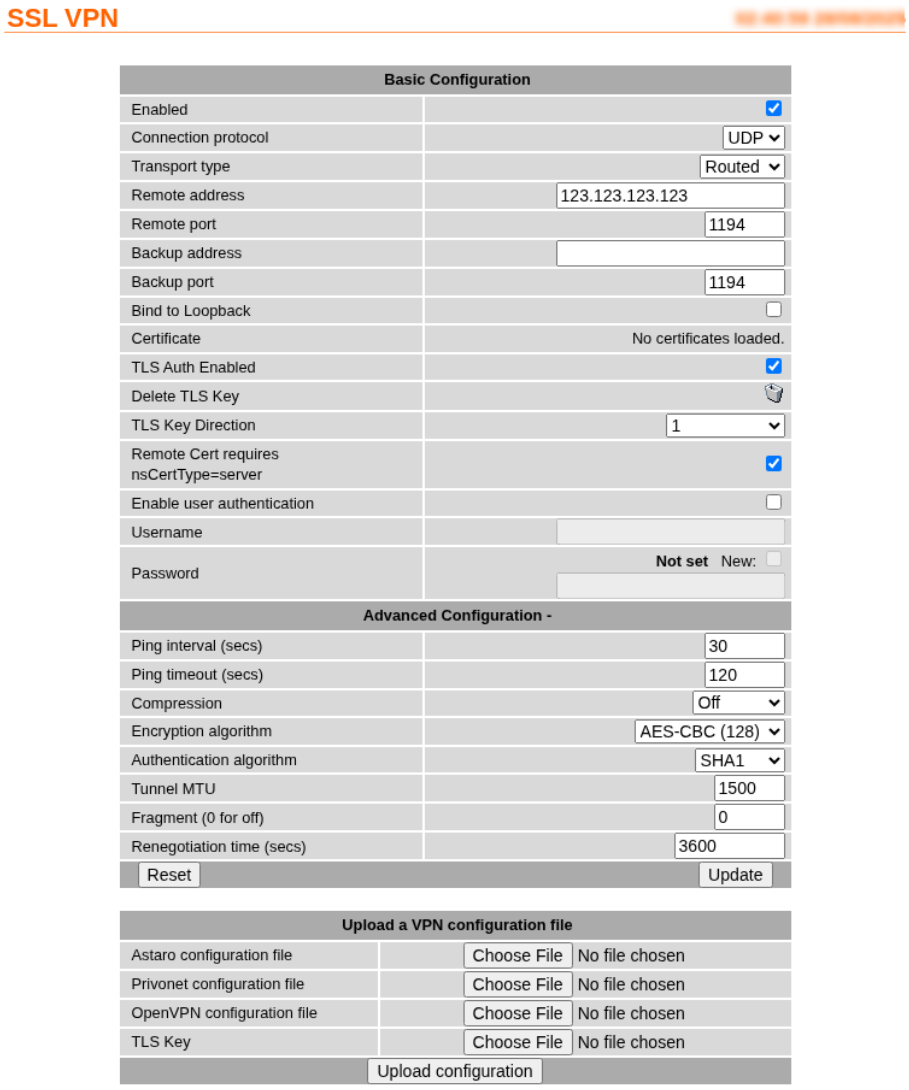


Fig. 11.43: SSL based VPN configuration web page.

Remote port
1194

Bind to Loopback
Un-checked.

Certificate
demoClient

Remote Cert requires nsCertType=server
Checked.

Enable user authentication
Un-checked

Username
Not required. Leave blank.

Password
Not required. Leave blank.

Advanced Configuration

Ping interval (secs)
30

Ping timeout (secs)
120

Compression
Off

Encryption algorithm
Blowfish (128)

Tunnel MTU
1500

Fragment (0 for off)
0

Renegotiation time (secs)
3600

Once the configuration has been completed click the Update button to save the changes.

The SSL VPN will now be started and it will attempt to establish a connection with the VPN server specified. The status of the VPN can be checked on the VPN status page. To access this page, click *Status* → *VPN*. A page similar to that shown in Fig. 11.44 will be shown. This page indicates that the VPN is connected and lists the local IP address.

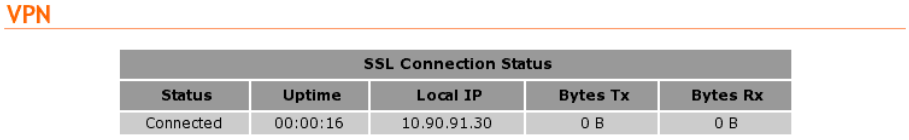


Fig. 11.44: SSL VPN status page.

In order to test the VPN a ping command can be run from a machine connected to the VPN server. The following is the result of the ping:

```
$ ping 10.90.91.30
PING 10.90.91.30(10.90.91.30) 56(84) bytes of data.
64 bytes from 10.90.91.30: icmp_seq=1 ttl=62 time=141 ms
64 bytes from 10.90.91.30: icmp_seq=2 ttl=62 time=122 ms
```

(continues on next page)

(continued from previous page)

```
64 bytes from 10.90.91.30: icmp_seq=3 ttl=62 time=120 ms
64 bytes from 10.90.91.30: icmp_seq=4 ttl=62 time=121 ms
64 bytes from 10.90.91.30: icmp_seq=5 ttl=62 time=121 ms
64 bytes from 10.90.91.30: icmp_seq=6 ttl=62 time=122 ms
64 bytes from 10.90.91.30: icmp_seq=7 ttl=62 time=123 ms
--- 10.90.91.30 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5998ms
rtt min/avg/max/mdev = 120.620/124.725/141.429/6.867 ms
```

The unit has responded to the ping and the byte counters on the status page have increased as seen in Fig. 11.45

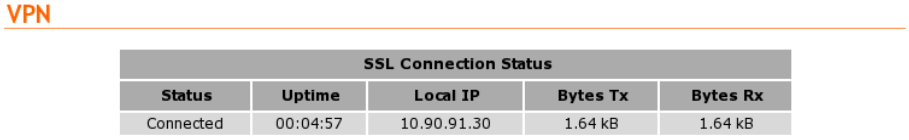


Fig. 11.45: SSL VPN status after running Ping, the byte counts have increased.

The VPN is now operational as can be used to pass data.

11.3 PPTP and L2TP

11.3.1 Point-to-Point-Tunneling-Protocol

The Point-to-Point-Tunneling-Protocol (PPTP) is used for establishing Virtual Private Network (VPN) tunnels over an insecure network such as the Internet. PPTP uses a client-server model for establishing the VPN. The unit provides a PPTP client. PPTP was developed by Microsoft and is provided with most versions of the Windows operating system. An advantage of PPTP is it is easy to configure.

11.3.2 Layer 2 Tunnel Protocol

The Layer 2 Tunnel Protocol (L2TP) is an Internet Engineering Task Force (IETF) standard which combines the best features of two existing tunnelling protocols, Layer 2 Forwarding (L2F) developed by Cisco and the Point-to-Point Tunnelling Protocol (PPTP). L2TP can be viewed as an extension to the Point-to-Point Protocol (PPP). One endpoint of an L2TP tunnel is called the L2TP Network Server (LNS), the LNS waits for new tunnels to be established. The other end-point is called the L2TP Access Concentrator (LAC), the LAC initiates tunnel connections to the LNS, the unit implements an L2TP LAC. Once the L2TP tunnel has been established the traffic over the tunnel is bidirectional.

11.3.3 PPTP and L2TP Configuration

To access the PPTP & L2TP configuration page select VPN . PPTP & L2TP a page similar to that shown in Fig. 11.46 will be displayed. The PPTP & L2TP page will list the currently configured tunnels.

L2TP Global Configuration Bind to Loopback
: Check to bind the service to the loopback port. Refer to the *Loopback Interface* section for details on configuring the loopback interface.

11.3.4 Add a PPTP or L2TP tunnel

To add a new PPTP or L2TP tunnel Click the Add new tunnel button. The Add new tunnel page will be displayed as shown in Fig. 11.47

Add new tunnel
: Options:

  Label
  : A label or name for the tunnel.

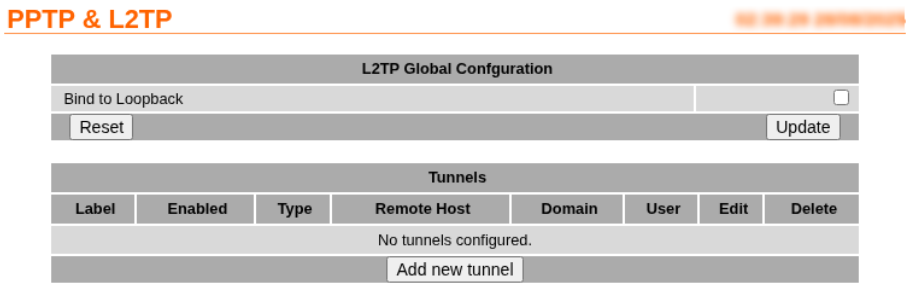


Fig. 11.46: The PPTP & L2TP main page.

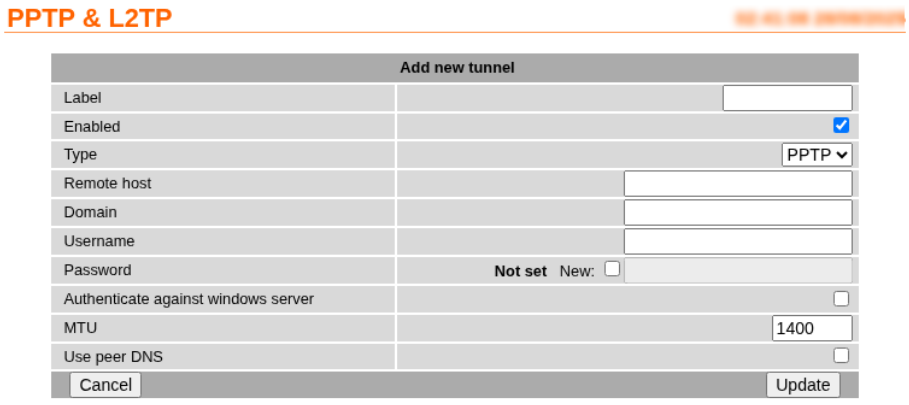


Fig. 11.47: The PPTP & L2TP Add new tunnel page.

Enabled
Check the box to enable the tunnel.

Type

Select the type of tunnel from the drop-down list, the options are:

PPTP
Point-to-Point Tunnelling Protocol

L2TP
Layer 2 Tunnelling Protocol

Remote host
Specify then IP address or fully qualified domain name of the remote host.

Domain
Specify the Windows network domain. (Optional)

Username
The user-name for authentication.

Password
Specify the password for connection with the remote host. To set a new password click the **New** check-box and then enter the password.

Authenticate against windows server
Check to enable authentication with a Windows server.

MTU
Specify the Maximum Transmission Unit (MTU), which is the size, in bytes, of the largest packet which can be sent over the PPTP / L2TP tunnel. The default value is 1400.

Use peer DNS
Check the box to enable peer DNS.

Click the Update button to save and commit changes.

11.3.5 PPTP configuration example

The following is an example of connecting a PPTP tunnel to a PPTP VPN server. Fig. 11.48 illustrates the network which will be established. For this example a connection will be established from the unit to a PPTP server. The tunnel will be called test, it is of type PPTP and the remote host is at IP address 123.123.123.123. The domain is test.com.au, the user-name is user and the password password. The MTU setting is left at the default of 1400 and peer DNS is enabled.

To access the PPTP & L2TP configuration page select *VPN → PPTP & L2TP* from the menu. The PPTP & L2TP page will then be displayed. To add a tunnel Click the Add new tunnel button on the main PPTP & L2TP page. The Add new tunnel page will be displayed. Fig. 11.49 illustrates the PPTP add tunnel page with the parameters entered for the configuration described above.

The following settings are used to configured the tunnel as described:

Label
Test

Enabled
On (Checked)

Type
PPTP

Remote host
123.123.123.123

Domain
x

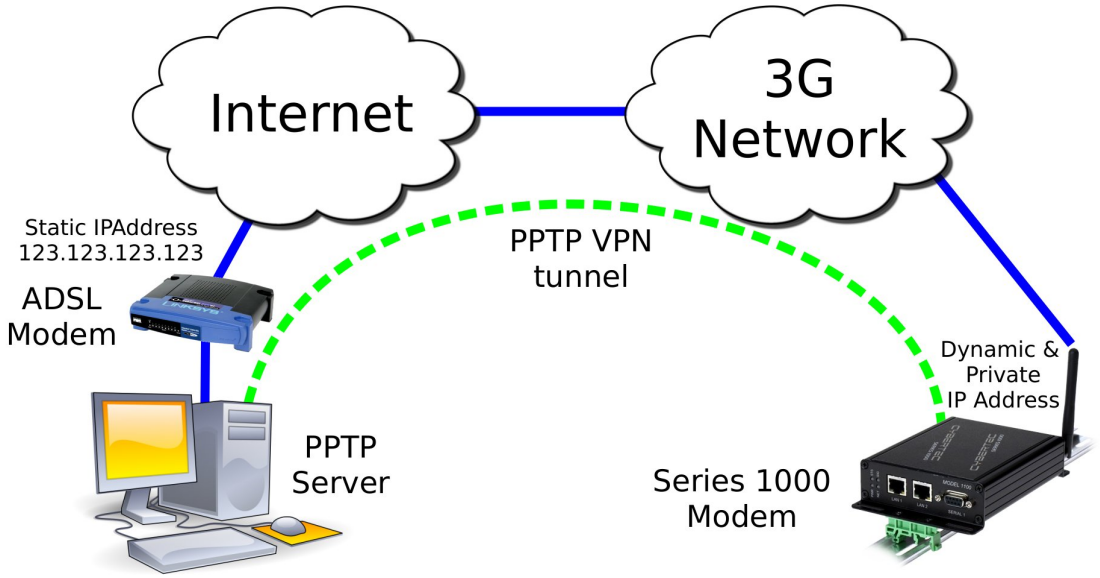


Fig. 11.48: PPTP based VPN example network.

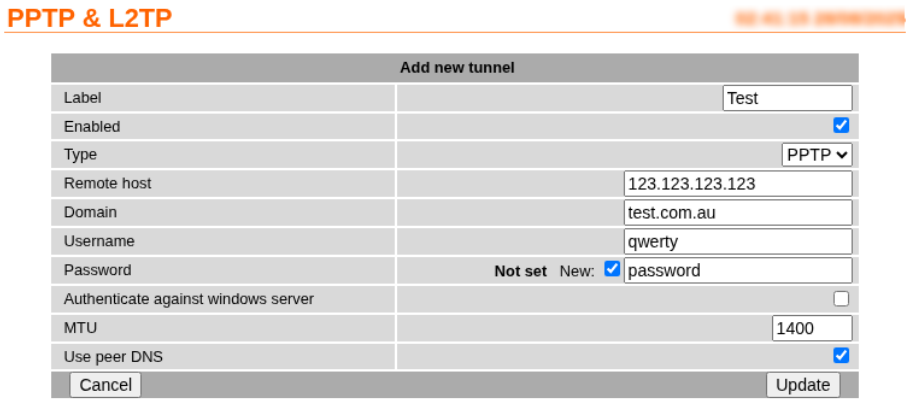


Fig. 11.49: The PPTP & L2TP main page.

Username
qwerty

Password
password

MTU
1400

Use peer DNS
On (Checked)

Once the options have been entered click the Update button to save and commit changes.

The settings will be saved and the main PPTP & L2TP page will be displayed with the new tunnel added to the Tunnels table, as shown in Fig. 11.50. The unit will now attempt to establish a connection with the PPTP server.

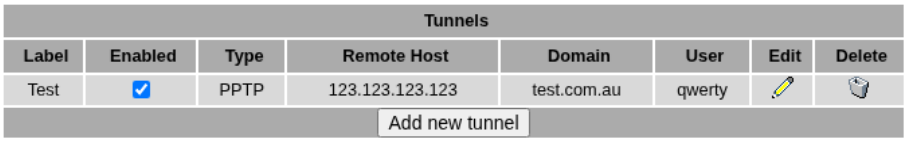


Fig. 11.50: The PPTP & L2TP main page.

To check the status of the page click *Status* → *VPN*. The VPN status page will then be displayed. Fig. 11.51 is the status page for the PPTP VPN created in this example.

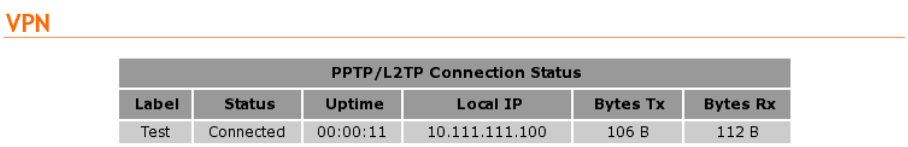


Fig. 11.51: The PPTP & L2TP status page.

The status of the tunnel is connected, indicating that the tunnel has been established and traffic can flow. The status page also indicates the local IP address of the tunnels and the number of bytes that have been received and transmitted.

11.4 Multiple VPN Tunnels

The total number of VPN tunnels support is model dependant. On models which support multiple VPN tunnels these can be configured to operate simultaneously. Fig. 11.52 is an example of the VPN Status page with one SSL, one IPsec and one PPTP VPN tunnel operating simultaneously.

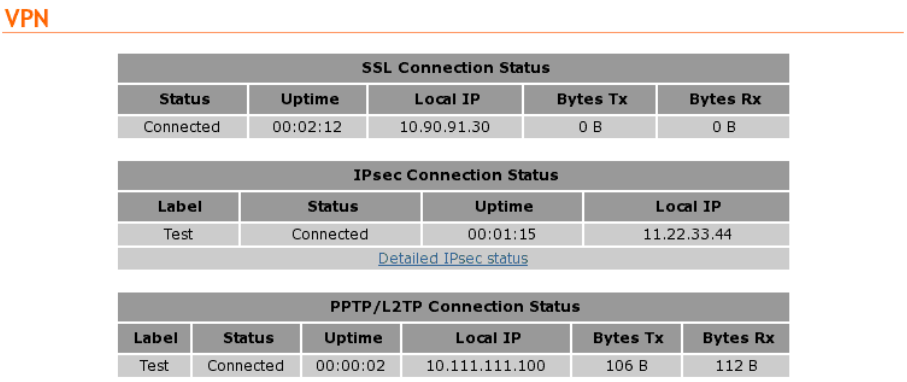


Fig. 11.52: The VPN status page showing 3 active VPN connections.

11.5 Certificate Management

Digital certificates are a form of digital identification used for authentication. A digital certificate contains information that identifies a device or user. They are issued in the context of a Public Key Infrastructure (PKI), which uses public-key/private-key encryption to ensure security. Support is provided for X.509 digital certificates (International Telecommunications Union Recommendation X.509), including SSL (Secure Sockets Layer) certificates.

To access the certificate management page select *VPN* → *Certificates* a page similar to that shown in Fig. 11.53 will be displayed. The top part of the page lists the currently loaded certificates, the second section is for uploading a new certificate and the last section is for configuring Simple Certificate Enrolment Protocol (SCEP).

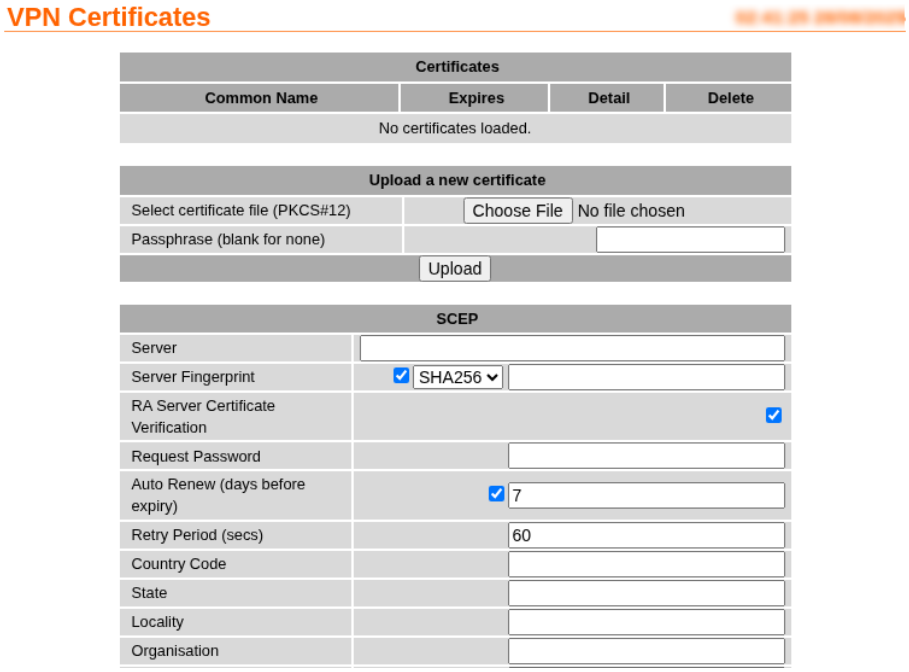


Fig. 11.53: VPN certificate management.

11.5.1 Add a certificate

To add a certificate click the Choose file button, then navigate to the certificate and select it. If a passphrase is required to read the certificate then it should be entered in the text box. To upload the certificate click the Upload configuration button.

In the example shown in Fig. 11.54, the file demoClient1.p12 is selected which contains the certificate demoClient. To select the certificate file click the Choose file button, then navigate to and select the certificate file demoClient1.p12, the file name will then be shown next to the Choose file button.

To upload the certificate click the Upload configuration button. The page will be updated and the certificate will be added to the Certificates table as shown in Fig. 11.55.

11.5.2 Checking the certificate details

Once uploaded the details of a certificate can be displayed by clicking the icon located in the detail column of the table. Fig. 11.56 is an example of the details of a certificate.

Click the OK button to return to the main certificate page.

Fig. 11.54: Uploading a VPN certificate.

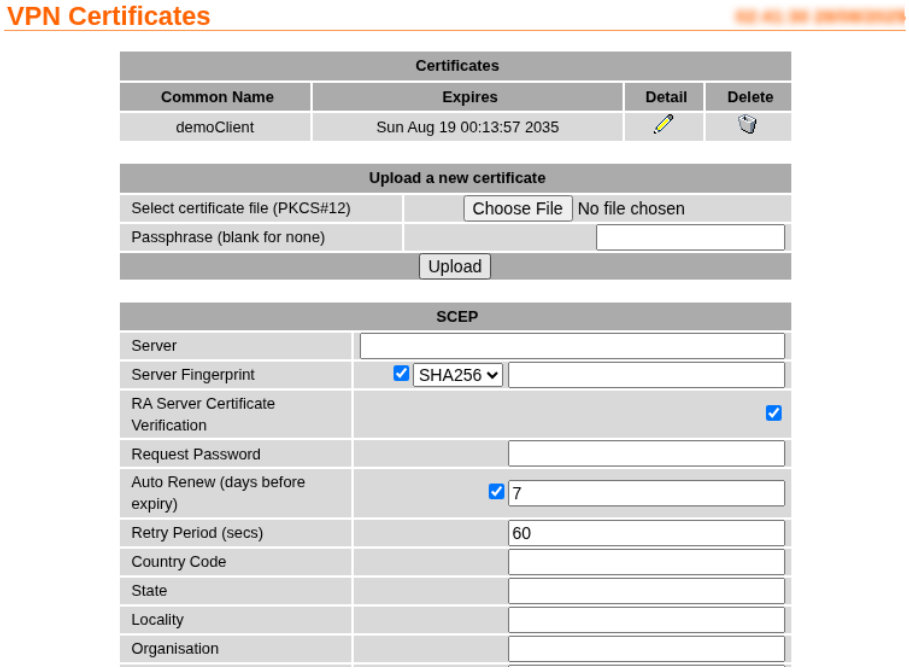


Fig. 11.55: VPN certificate table listing the uploaded certificate.

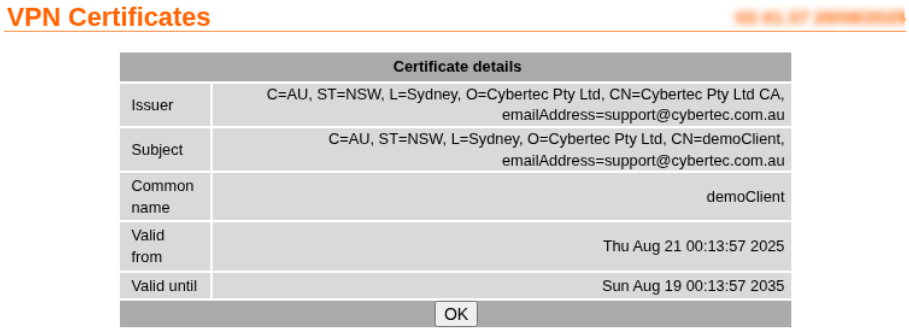


Fig. 11.56: VPN certificate details.

11.5.3 Adding further certificates

Additional certificates can be uploaded using the same process. For each additional certificate click the Choose file button, navigate to the certificate then click the Upload configuration button.

In the example shown in Fig. 11.57, the file demoClient2.p12 is selected which contains the certificate demoClient2. To select the certificate file click the Choose file button, then navigate to and select the certificate file demoClient2.p12, the file name will then be shown next to the Choose file button.

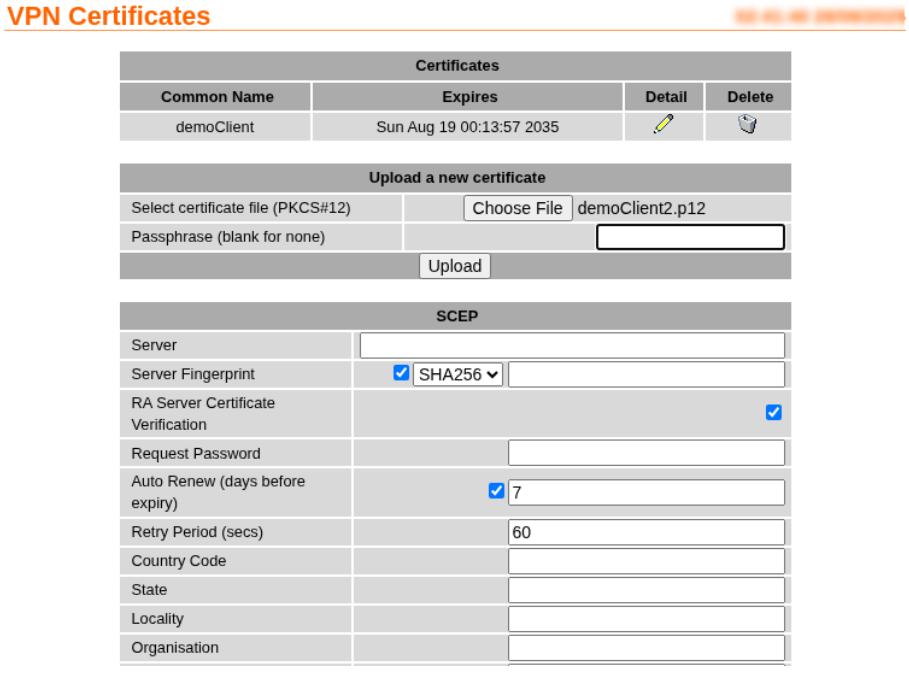


Fig. 11.57: Adding a second VPN certificate.

To upload the certificate click the Upload configuration button. The page will be updated and the certificate will be added to the Certificates table as shown in Fig. 11.58.

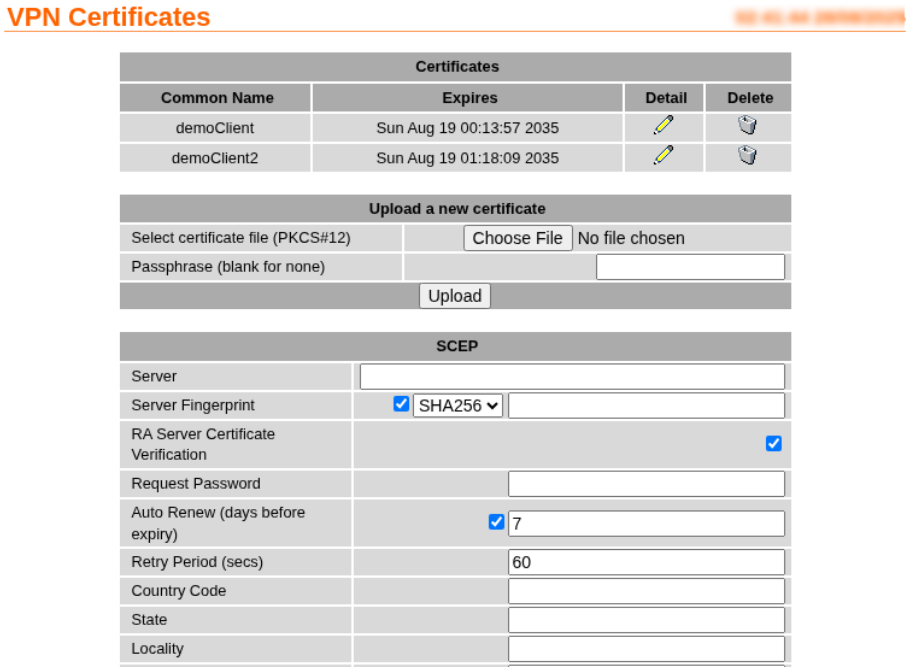


Fig. 11.58: VPN certificate table listing both uploaded certificates.

11.5.4 Deleting a certificate

A certificate can be deleted by clicking the icon in the **Delete** column of the certificate to be deleted. When the icon is clicked a warning box will be displayed. Click the OK button to confirm the deletion or click the Cancel button to prevent the certificate from being deleted.

For example, to delete certificate 2 from the table shown in Fig. 11.58, click the icon in row 2 of the table. A warning box will now be displayed as shown in Fig. 11.59, click the OK button and the certificate will be deleted.

The certificate table will be update and the certificate removed, as shown in Fig. 11.60.

11.5.5 Simple Certificate Enrolment Protocol (SCEP)

The Simple Certificate Enrolment Protocol (SCEP), is a protocol which enables a client, which employs Public Key Infrastructure (PKI), to request, renew, update and revoke a certificate from a Certification Authority (CA).

The parameters for SCEP are in a table in the lower section of the main certificate page as shown in Fig. 11.61.

Note

Not all parameters are required for SCEP to function. As a minimum the Server address and common name are required.

The number of parameters specified will be determined by the way in which the server has been configured.

SCEP

Configuration as follows:

Server

The IP address or URL of the Certificate server.

Server Fingerprint

The server finger print:

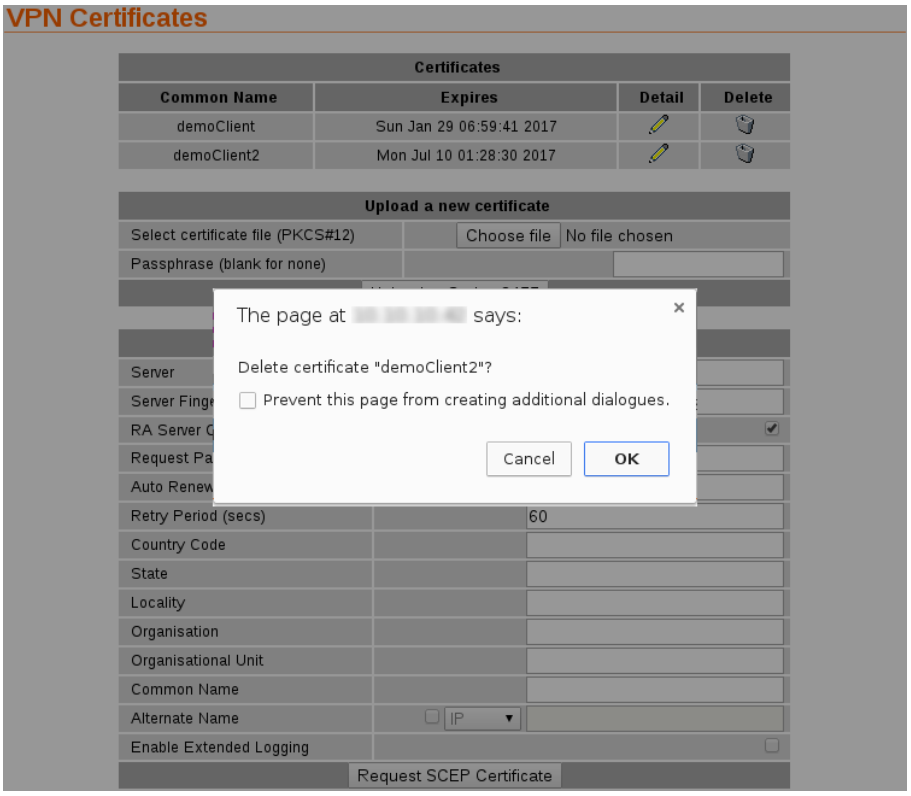


Fig. 11.59: Deleting a VPN certificate.

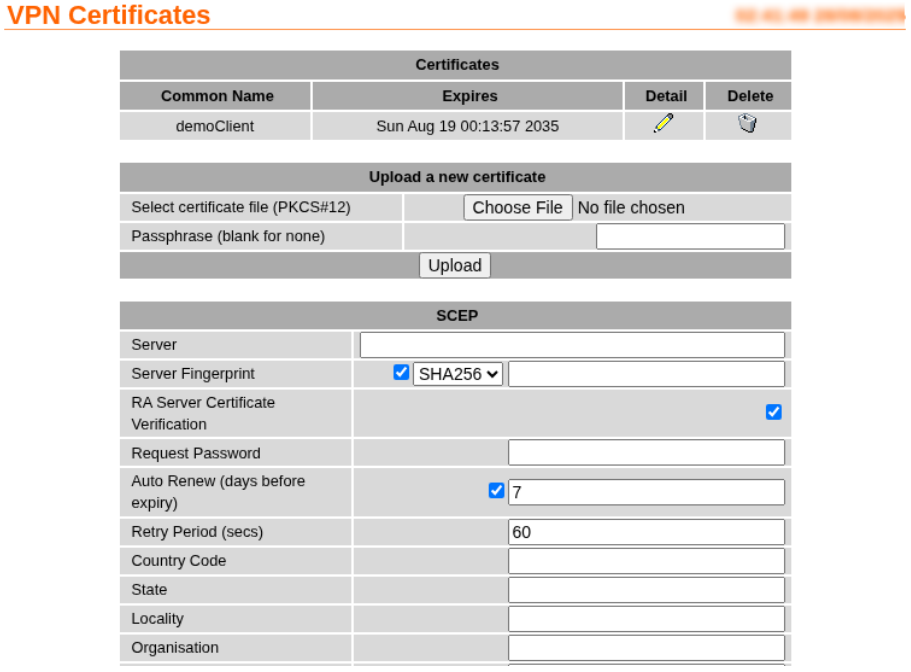


Fig. 11.60: VPN certificate list with the second certificate deleted.

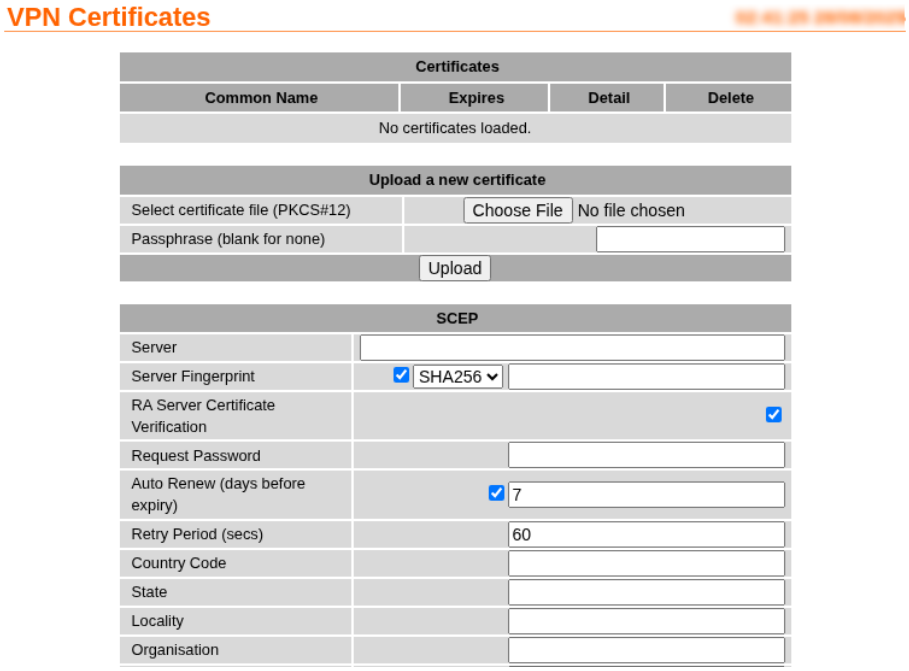


Fig. 11.61: VPN certificate SCEP configuration.

Enable
Check to enable

Hash
Select the hash algorithm from the drop-down list.

MD5
Message-Digest algorithm 5.

SHA1
Secure Hash Algorithm 1.

SHA224
Secure Hash Algorithm 2 (224 bit).

SHA256
Secure Hash Algorithm 2 (256 bit).

SHA384
Secure Hash Algorithm 2 (384 bit).

SHA512
Secure Hash Algorithm 2 (512 bit).

Fingerprint
Enter the server fingerprint to use.

RA Server Certificate Verification
Check to enable.

Request Password
The request password.

Auto Renew (days before expiry) Enable
Check to enable automatic request for certificate renewal.

Days
Enter the number of days prior to expiry to request certificate renewal.

Retry Period
Enter the number of seconds after which to re-try a failed server connection attempt.

Country Code
Enter the country code.

State
Enter the state.

Organisation
Enter the organisation name.

Organisational Unit
Enter the name of the organisational unit.

Common Name
Enter the common name of the certificate.

Alternate Name
The alternate name:

Enable
Check to enable.

Type
Select from IP address or Fully Qualified Domain Name (FQDN).

Key Length
Select the key length from the drop-down list. The options are:

- 1024
- 2048
- 4096

The default is: 1024

String Encoding
Select the string encoding from the drop-down list. The options are:

- UTF8
- ASCII

The default is: UTF8

CSR Signature Algorithm
Select the CSR signature algorithm from the drop-down list. The options are:

MD5
Message-Digest algorithm 5.

SHA1
Secure Hash Algorithm 1.

SHA224
Secure Hash Algorithm 2 (224 bit).

SHA256
Secure Hash Algorithm 2 (256 bit).

SHA384
Secure Hash Algorithm 2 (384 bit).

SHA512
Secure Hash Algorithm 2 (512 bit).

The default is: SHA256

Enable Extended Logging

Check to enable extending logging.

This provide more detail in the logs and is useful for debugging. It is not recommended for production use as it can be verbose.

Click the Request SCEP Certificate button to request a certificate from the certificate server.

CHAPTER

TWELVE

SERIAL SERVER

The serial server is used to transfer data between a physical serial port and an IP connection. The IP connection can be via the Ethernet or the wireless connection of the modem. The remote host that connects to the serial server could be a SCADA master, desktop PC or even another modem.

The Serial Server configuration page is accessed by selecting the *Serial Server* tab from the main menu. When selected a page similar to that shown in Fig. 12.1 will be displayed.

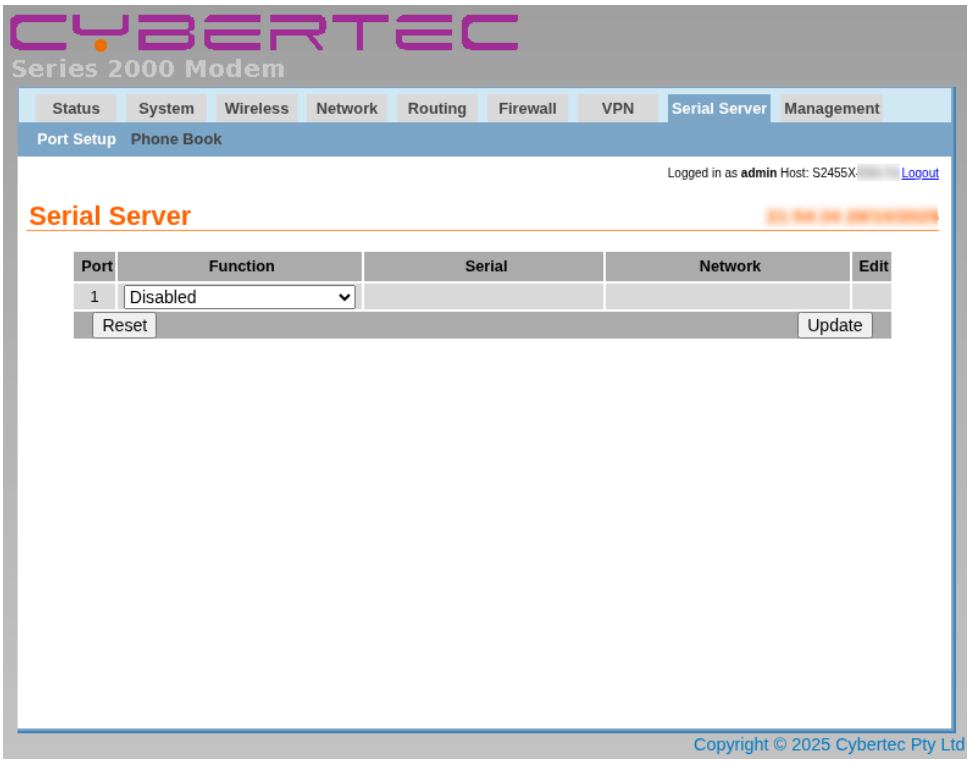


Fig. 12.1: Serial server main page for model with 1 serial port.

For models with more than 1 serial port the Serial Server page will look similar to that shown in Fig. 12.2

12.1 Selecting a port function

Each port of the serial server can be configured to operate with a different function. The function selected for an application will be determined by the serial equipment attached to the port and the type of IP connection required. To display the Serial Server Port Setup page select *Serial Server* → *Port Setup* from the menu.

The page shown will differ slightly between models, Fig. 12.3 is an example page from a unit with a single serial port, while Fig. 12.4 is an example page from a unit with 3 serial ports.

The table provides a summary of the port settings. The columns have the following meanings:

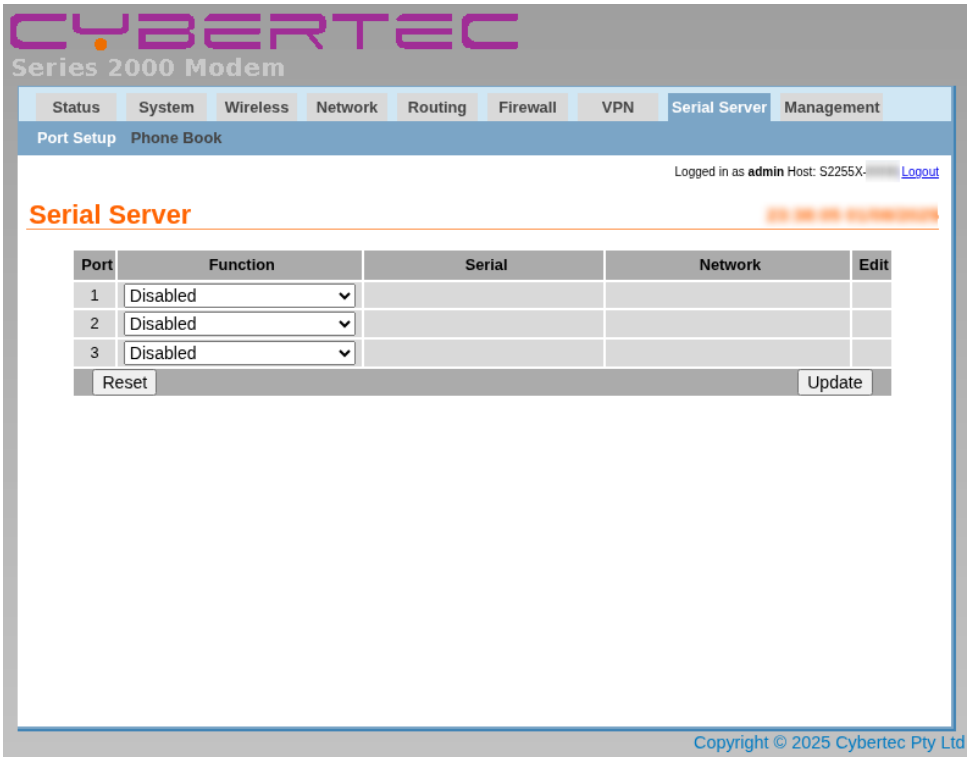


Fig. 12.2: Serial server main page for model with 3 serial ports.

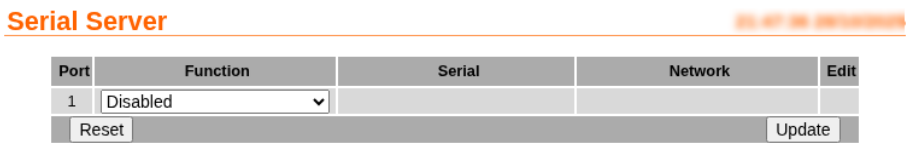


Fig. 12.3: Serial server main page for model with 1 serial port.

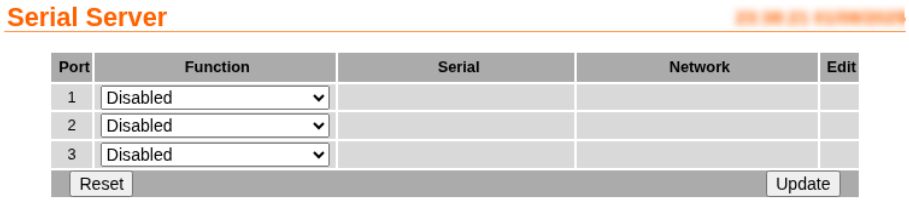


Fig. 12.4: Serial server main page for model with 3 serial ports.

Port
The port number corresponds to the physical port number. Refer to the hardware manual for the model being configured for details.

Function
The port function, the following options are available:

Disabled
Serial server functionality is disabled for the port.

Raw TCP Client/Server
The serial server function will create a transparent pipe between the serial port and a TCP network connection. Example uses of this mode include connecting to a remote PC running serial port redirector software with virtual COM ports or connecting two modems back-to-back to create a serial bridge.

Raw UDP
This function is similar to Raw TCP Client/Server mode, but uses UDP as the network transport. UDP has lower overheads than TCP, but as UDP offers no lost packet detection, this function should only be used with serial protocols that can provide the necessary error correction.

Raw TCP MUX
This function is similar to Raw TCP Client/Server mode, but allows multiple TCP connections to be established to the serial port. This allows multiple remote hosts to connect to the serial port. The connections can be established in either direction, allowing the serial port to be used as a TCP server or client.

Raw UDP MUX
This function is similar to Raw UDP mode, but allows multiple UDP connections to be established to the serial port. This allows multiple remote hosts to connect to the serial port.

Modem Emulator
The serial server provides an AT command interface at the serial port that simulates a traditional dial-up modem. However, instead of dialling out phone calls, the emulator creates TCP network connections. The emulator will also simulate incoming calls if it receives a TCP connection. The function is suited to applications where equipment attached to the serial port expects to see a dial-up modem.

DNP3 IP-Serial Gateway
The serial server will act as a DNP3 outstation to be polled by a SCADA master. The outstation mode is configurable as a TCP listen endpoint, TCP dual-function endpoint or UDP endpoint.

Modbus IP-Serial Gateway
The serial server will perform conversion from Modbus/TCP to Modbus/RTU or Modbus/ASCII, allowing polling by a Modbus/TCP master.

Telnet (RFC2217) Server
The serial server will function as a Telnet server, including the protocol extensions defined in RFC 2217. In addition to transporting data, this mode also allows a remote PC with appropriate software to change the port configuration (baud rate etc) and read and write the handshaking lines during a session.

PPP Server
The port acts as a PPP server. A device is able to connect to the port and establish a PPP session. Once established the connection acts in a similar way to other packet interfaces.

PPP Dialout Client
The port establishes a connection to a PPP server. Once established the connection acts in a similar way to other packet interfaces.

Serial
The serial port parameters. Listed in the form:

<baud> <data bits><parity><stop bits>

For example: 19200 8N1 indicates a baud rate of 19200, 8 data bits, Non parity and 1 stop bit.

For details on configuring the port parameters refer to *Serial port settings*.

Network
The network parameters associated with the port. The parameters listed will depend on the mode in which the port is operating.

Click the Update button to save and commit the selected function.

The port options can be edited by clicking the  icon for the associated port.

12.2 Common configuration options

12.2.1 Serial port settings

Regardless of the selected port function, each port needs to be configured to match the parameters of the equipment attached to the port. As the configuration of a port function is edited, the port options will be displayed as shown in Fig. 12.5 for DCE type ports or Fig. 12.6 for DTE type ports.

Port Configuration	
Port Type	DCE
Baudrate	19200
Data bits	8
Stop bits	1
Parity	None
Flow control	None
Assert control signal when disconnected	CTS DSR
Network congestion backoff signal	CTS DSR

Fig. 12.5: Common port configuration parameters for DCE type port.

Port Configuration	
Port Type	DTE
Baudrate	28800
Data bits	8
Stop bits	1
Parity	None
Flow control	None
Assert control signal when disconnected	RTS DTR
Network congestion backoff signal	RTS DTR

Fig. 12.6: Common port configuration parameters for DTE type port.

For each port, the following parameters are available:

Port Configuration

Port Type (read only)
Reports the serial port type, either DCE or DTE.

The type of port determines which control lines are outputs.

- for DCE type ports the control lines which are outputs are CTS and DSR.
- for DTE type ports the control lines which are outputs are RTS and DTR.

Baudrate
The port can be configured for any standard baud-rate from 300 baud to 230400 baud.

Data bits
The port can be configured for operation with 5 to 8 data bits.

Stop bits
The port can be configured for operation with 1 or 2 stop bits.

Parity
The port can be configured for none, odd or even parity.

Flow control
The serial server port can be configured for the following modes:

None
No flow control is enabled.

Hardware
The port will use the RTS and CTS handshake lines to control the flow of data.

Software
The port will use XON/XOFF software flow control. The XOFF character is hex 0x13. The XON character is hex 0x11.

Both
The port will use both hardware and software flow control.

Assert control signal when disconnected
This field determines the state of the serial port control lines while the port is disconnected.

To set a signal active while disconnected, check the box associated with the signal name.

Network congestion backoff signal
This field determines which control line or lines will be asserted when the network is congested and no further data is to be sent.

To set a signal to be asserted, check the box associated with the signal name.

12.2.2 Packet framer settings

The packet framer is available for port functions that carry raw data. The settings are not available for the protocol based functions such as DNP3 IP-Serial Gateway or Modbus IP-Serial Gateway as the packetisation is determined by the protocol.

The packet framer allows data received from the serial port to be packetised in a way consistent with the data being sent and received. This can reduce the overhead incurred in sending and receiving the data and can assist with reducing latency.

Fig. 12.7 shows the configuration options for the packet framer.

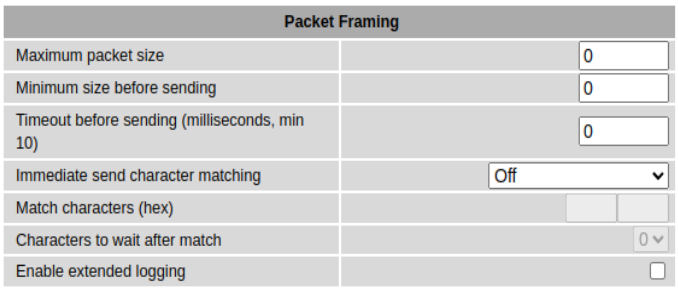


Fig. 12.7: Packet framing configuration options

The following packet framer options are available:

Packet Framing

Maximum packet size
This value determines the largest packet size to be passed to the network for transmission. If set to 0, the packet framer will be disabled and data will bypass the packet framer. The value chosen will depend on the application, however, the value should not be set higher than 1024, so as to ensure the packet will fit a conventional Ethernet frame.

Minimum size before sending
In some applications, it may not be desirable to wait for the exact number of bytes specified in **Maximum packet size** before sending the packet. The value set in this field, which must be less than or equal to the **Maximum packet size**, acts as a send threshold. Once the accumulated byte count reaches this value, the packet will be sent.

Timeout before sending
The time-out allows data accumulated by the framer to be sent after a specified period of serial receive inactivity. This prevents data from being held in the framer indefinitely should no more data arrive on the serial port. The time-out value is in milliseconds, with the minimum value being 10 milliseconds.

Immediate send character matching
This field allows the framer to be configured so that if certain characters are received the accumulated data is immediately sent. The character matching can function in one of the following modes:

Off
No character matching is done.

Match any character
If either of the characters set in the **Match characters** field are received, the data will be sent immediately.

Match all characters
If both of the characters set in the **Match characters** field are received in the order specified, the data will be sent immediately.

Match characters
Used in conjunction with the **Immediate send character matching** field, these characters determine what data will cause an immediate send. The values are entered as a hex value, so, for example, a newline (ASCII 10) would be entered as 0A. To delete a value, clear the text in the field.

Characters to wait after match
Used in conjunction with the **Immediate send character matching** field, this count determines how many additional characters will be received after an immediate match character is detected. This is useful if for example trailing characters always follow the match character.

Enable extended logging
Check box to enable debugging information to be written to the log file. This can be useful to assist when first configuring the packet framer settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

12.3 Raw TCP Client/Server

12.3.1 Description

The serial server will function to create a transparent pipe between the serial port and a TCP network connection. Example uses of this mode include connecting to a remote PC running serial port redirector software with virtual COM ports or connecting two modems back-to-back to create a serial bridge.

12.3.2 Selecting the port function

The serial server configuration is accessed by selecting *Serial Server → Port Setup*. To enable a port for the Raw TCP Client/Server function, select **Raw TCP Client/Server** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.8.

12.3.3 Configuring the port function

Once the port function has been selected, click on the  icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.9 will be displayed.

The following options can be set:

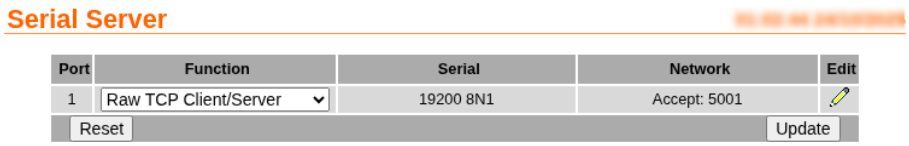


Fig. 12.8: Selecting Raw TCP Client/Server function

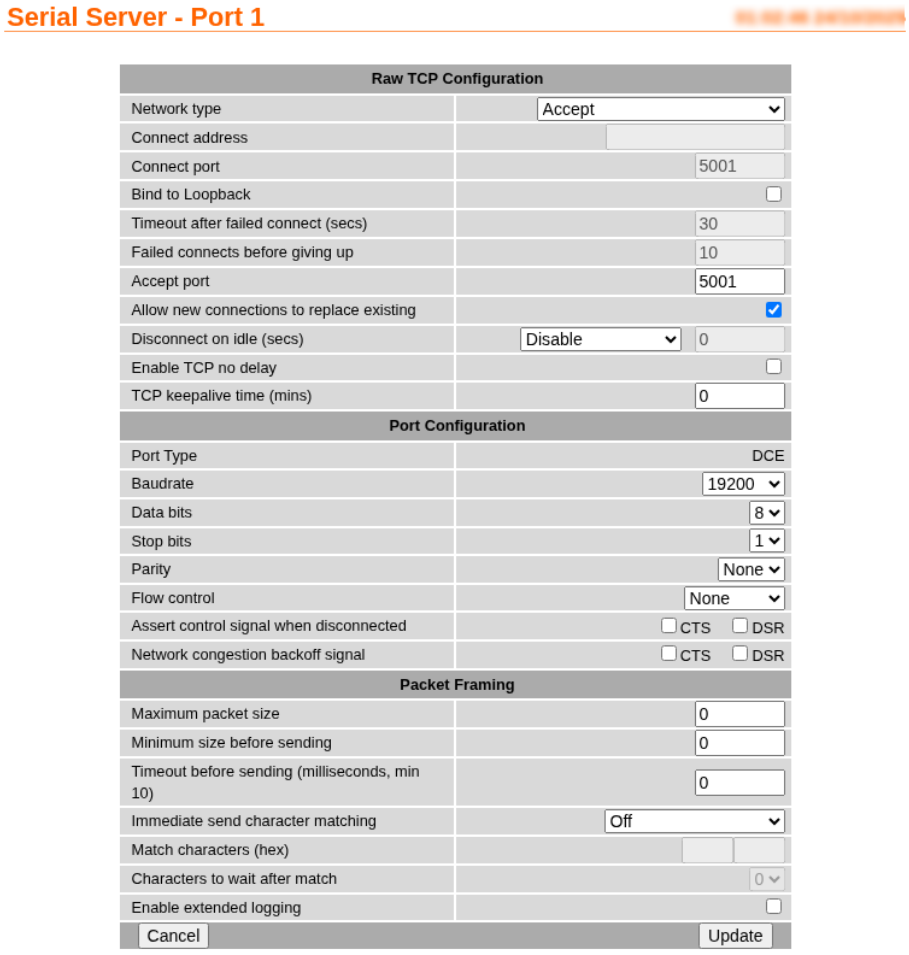


Fig. 12.9: Raw TCP Client/Server configuration

Raw TCP Client/Server

Network type

The Raw TCP serial server can be configured for three different network modes:

Connect

The serial server will establish a TCP connection to the specified address and port number.

Accept

The serial server will listen for TCP connections on the specified port number.

Connect on demand

The serial server will establish a TCP connection to the specified address and port number when data is received at the serial port and no connection exists.

Accept & connect on demand

The serial server will normally listen for TCP connections on the specified port number, however if data is received at the serial port and no connection exists, it will attempt to establish a connection to the specified address and port number.

Connect address

For **Connect**, **Connect on demand** or **Accept and Connect on demand** network modes, this is the address the server will attempt to connect to. The address entered should be in IPv4 decimal dotted notation.

Connect port

For **Connect** or **Accept and Connect** network modes, this is the TCP port number the server will attempt to connect to. The value entered should be a valid TCP port number.

Bind to Loopback

Check to bind the service to the loopback port.

Refer to the *Loopback Interface* section for details on configuring the loopback interface.

Timeout after failed connect

For **Connect** or **Accept and Connect** network modes, if a connection request has failed, the server will wait the amount of time (in seconds) specified in this field before attempting another connection request. While a short time-out may cause the connection to be established more quickly, it may also cause greater network traffic if the remote host is unavailable and repeated attempts fail.

Failed connects before giving up

For **Accept and Connect** network modes, the serial server will attempt to establish a connection for the number of times specified in this field by giving up and waiting for a connection to be accepted.

Accept port

For **Accept** or **Accept and Connect** network modes, this is the TCP port number on which the server will listen for connections.

Allow new connections to replace existing

For **Accept** or **Accept and Connect on demand** network modes, if a TCP connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Disconnect on idle

Controls whether and when the serial server closes an idle TCP connection. The mode dropdown selects what counts as idle; the seconds textbox sets the inactivity threshold. There are four modes to choose from:

Disable

The serial server will not close the connection due to inactivity.

Any data

The serial server will close the connection if no data has been received for the specified number of seconds.

Data to serial port
The serial server will close the connection if no data has been received for the specified number of seconds and no data has been sent to the serial port.

Data to network
The serial server will close the connection if no data has been received for the specified number of seconds and no data has been received from the network.

Enable TCP no delay
Check to enable TCP no delay.

> **Note**
>
> TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once.
>
> For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reasons that it is not recommended to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

TCP keepalive time
When set to a value greater than 0, TCP keep-alives will be enabled for connections, with probes sent at the frequency specified (minutes). This may assist in detecting failed connections.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Packet Framing
For information on setting the Packet Framing, refer to *Packet framer settings*.

Click the Update button to save and commit any configuration changes.

12.4 Raw UDP

12.4.1 Description

This function is similar to Raw TCP Client/Server mode, but uses UDP as the network transport. UDP has lower overheads than TCP, but as UDP offers no lost packet detection, this function should only be used with serial protocols that can provide the necessary error correction.

12.4.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the submenu. To enable a port for Raw UDP function, select **Raw UDP** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.10.

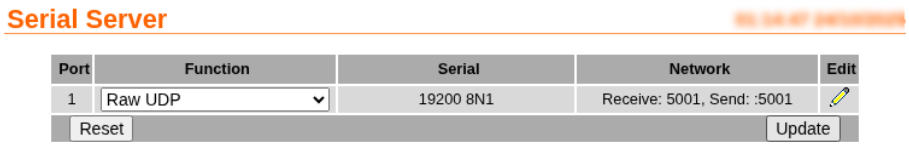


Fig. 12.10: Selecting Raw UDP function

12.4.3 Configuring the port function

Once the port function has been selected, click on the  icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.11, will be displayed.

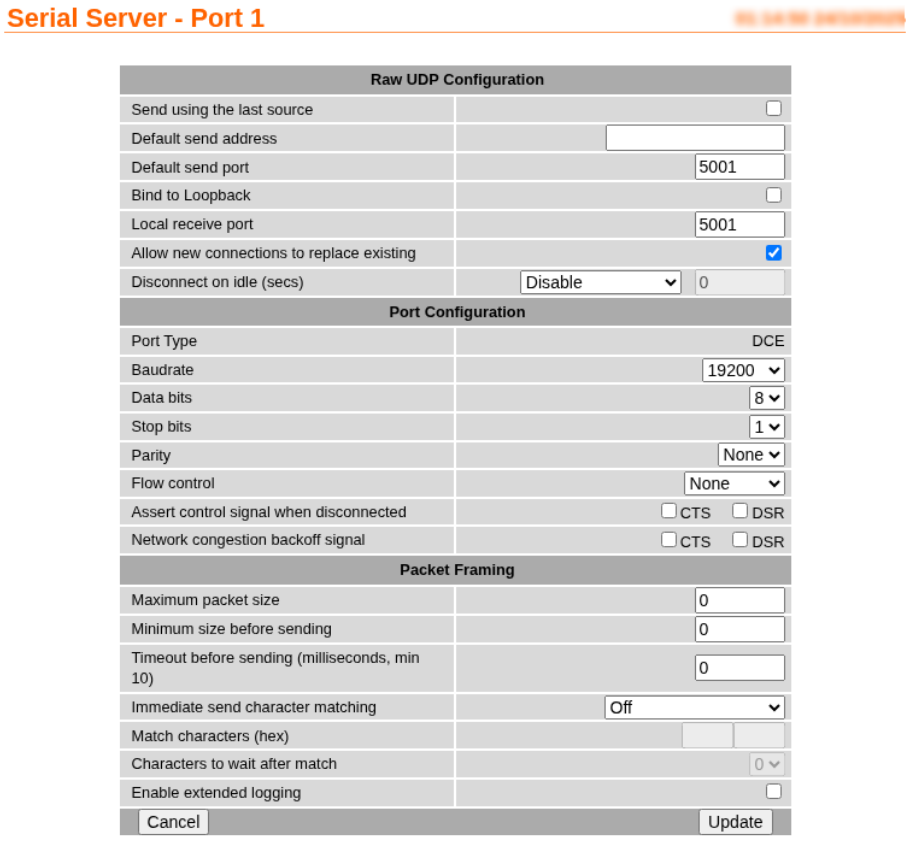


Fig. 12.11: Raw UDP configuration

The following options can be set:

Raw UDP Configuration

Send using the last source
Check to use the last received packet's source address and port number as the send address and port number.

Default send address
The default IP address the serial server will send UDP packets to. The address entered should be in IPv4 decimal dotted notation.

Default send port
The default UDP port number the server will send UDP packets to. The value entered should be a valid UDP port number.

Bind to Loopback
Check to bind the service to the loopback interface.

Refer to the *Loopback Interface* section for details on configuring the loopback interface.

Local receive port
This is the UDP port number that UDP packets will be received on at the modem. The value entered should be a valid UDP port number.

Allow new connections to replace existing
If a UDP packet is received and a connection is currently active on the serial server, this field determines

the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Disconnect on idle
Controls whether and when the serial server closes an idle TCP connection. The mode dropdown selects what counts as idle; the seconds textbox sets the inactivity threshold. There are four modes to choose from:

Disable
The serial server will not close the connection due to inactivity.

Any data
The serial server will close the connection if no data has been received for the specified number of seconds.

Data to serial port
The serial server will close the connection if no data has been received for the specified number of seconds and no data has been sent to the serial port.

Data to network
The serial server will close the connection if no data has been received for the specified number of seconds and no data has been received from the network.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Packet Framing
For information on setting the Packet Framing, refer to *Packet framer settings*.

Click the Update button to save and commit any configuration changes.

12.5 Raw TCP MUX

12.5.1 Description

This function is similar to Raw TCP Client/Server mode, but allows multiple TCP connections to be established to the serial port. This allows multiple remote hosts to connect to the serial port. The connections can be established in either direction.

12.5.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the submenu. To enable a port for the Raw TCP MUX function, select **Raw TCP MUX** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.12.

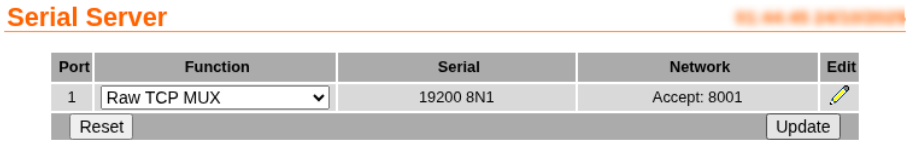


Fig. 12.12: Selecting Raw TCP MUX function

12.5.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.13, will be displayed.

The following options can be set:

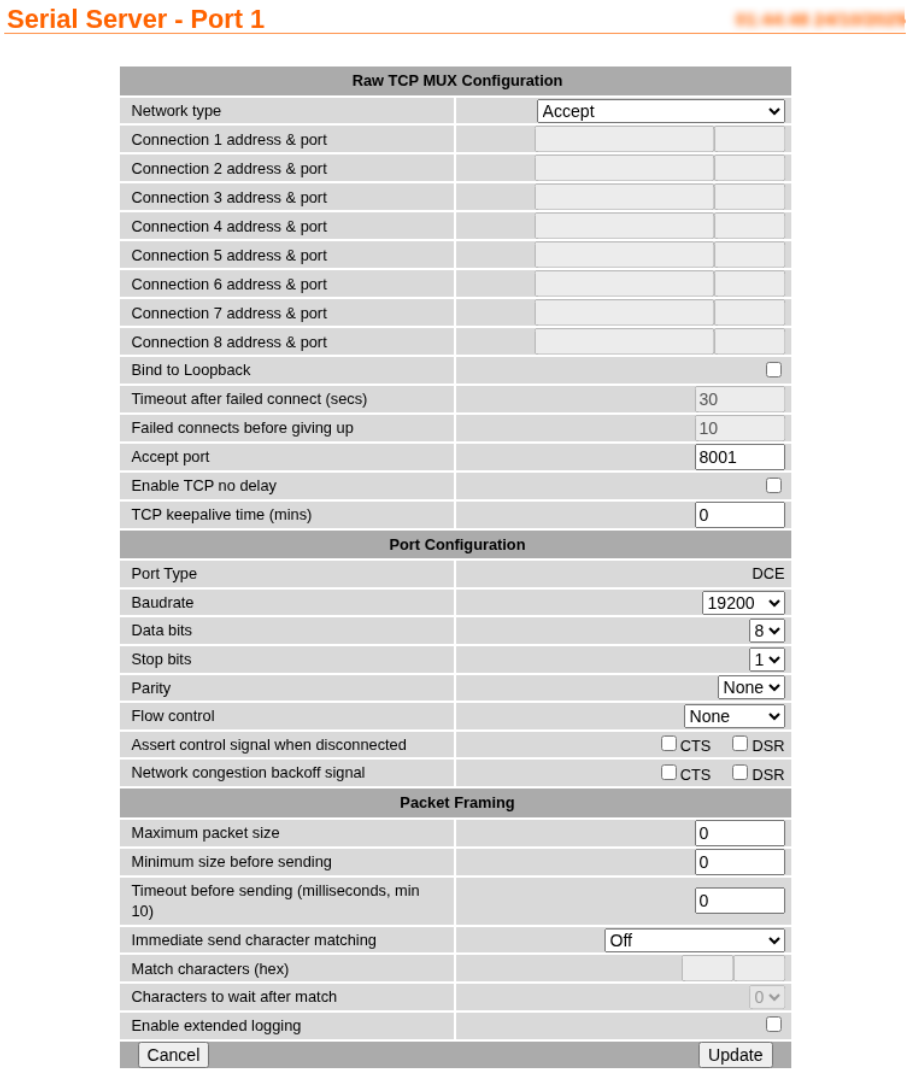


Fig. 12.13: Raw TCP MUX configuration

Raw TCP MUX Configuration

Network type
The Raw TCP MUX serial server can be configured for four different network modes:

Accept
The serial server will listen for TCP connections on the specified port number.

Connect
The serial server will establish TCP connections to the specified addresses and port numbers.

Connect on demand
The serial server will establish TCP connections to the specified addresses and port numbers when data is received at the serial port and no connections exist.

Accept & connect on demand
The serial server will normally listen for TCP connections on the specified port number, however, if data is received at the serial port and no connections exist, it will attempt to establish connections to the specified addresses and port numbers.

Connection 1-8 address & port
For **Connect**, **Connect on demand** or **Accept and Connect on demand** network modes, these fields allow up to 8 different TCP connections to be configured. Each connection can have its own IP address and port number. The addresses entered should be in IPv4 decimal dotted notation and the port values should be valid TCP port numbers.

Bind to Loopback
Check to bind the service to the loopback interface.

Refer to the *Loopback Interface* section for details on configuring the loopback interface.

Timeout after failed connect
For **Connect** or **Accept and Connect** network modes, if a connection request has failed, the server will wait the amount of time (in seconds) specified in this field before attempting another connection request. While a short time-out may cause the connection to be established more quickly, it may also cause greater network traffic if the remote host is unavailable and repeated attempts fail.

Failed connects before giving up
For **Accept and Connect** network modes, the serial server will attempt to establish a connection for the number of times specified in this field before giving up and waiting for a connection to be accepted.

Accept port
For **Accept** or **Accept and Connect** network modes, this is the TCP port number on which the server will listen for connections.

Enable TCP no delay
Check to enable TCP no delay.

> **Note**
>
> TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once.
>
> For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reasons that it is not recommended to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

TCP keepalive time
When set to a value greater than 0, TCP keep-alives will be enabled for connections, with probes sent at the frequency specified (minutes). This may assist in detecting failed connections.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Packet Framing
For information on setting the Packet Framing, refer to *Packet framer settings*.

Click the Update button to save and commit any configuration changes.

12.6 Raw UDP MUX

12.6.1 Description

This function is similar to Raw TCP MUX mode, but uses UDP as the network transport and allows multiple UDP connections to be established to the serial port. UDP has lower overheads than TCP, but as UDP offers no lost packet detection, this function should only be used with serial protocols that can provide the necessary error correction.

12.6.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the submenu. To enable a port for Raw UDP MUX function, select **Raw UDP MUX** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.14.

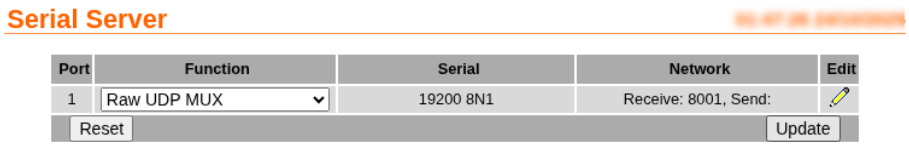


Fig. 12.14: Selecting Raw UDP MUX function

12.6.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.15, will be displayed.

The following options can be set:

Raw UDP MUX Configuration

Connection 1-8 address & port
These fields allow up to 8 different UDP connections to be configured. Each connection can have its own IP address and port number. The addresses entered should be in IPv4 decimal dotted notation and the port values should be valid UDP port numbers.

Bind to Loopback
Check to bind the service to the loopback interface.

Refer to the *Loopback Interface* section for details on configuring the loopback interface.

Local receive port
This is the UDP port number that UDP packets will be received on at the modem. The value entered should be a valid UDP port number.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Packet Framing
For information on setting the Packet Framing, refer to *Packet framer settings*.

Click the Update button to save and commit any configuration changes.

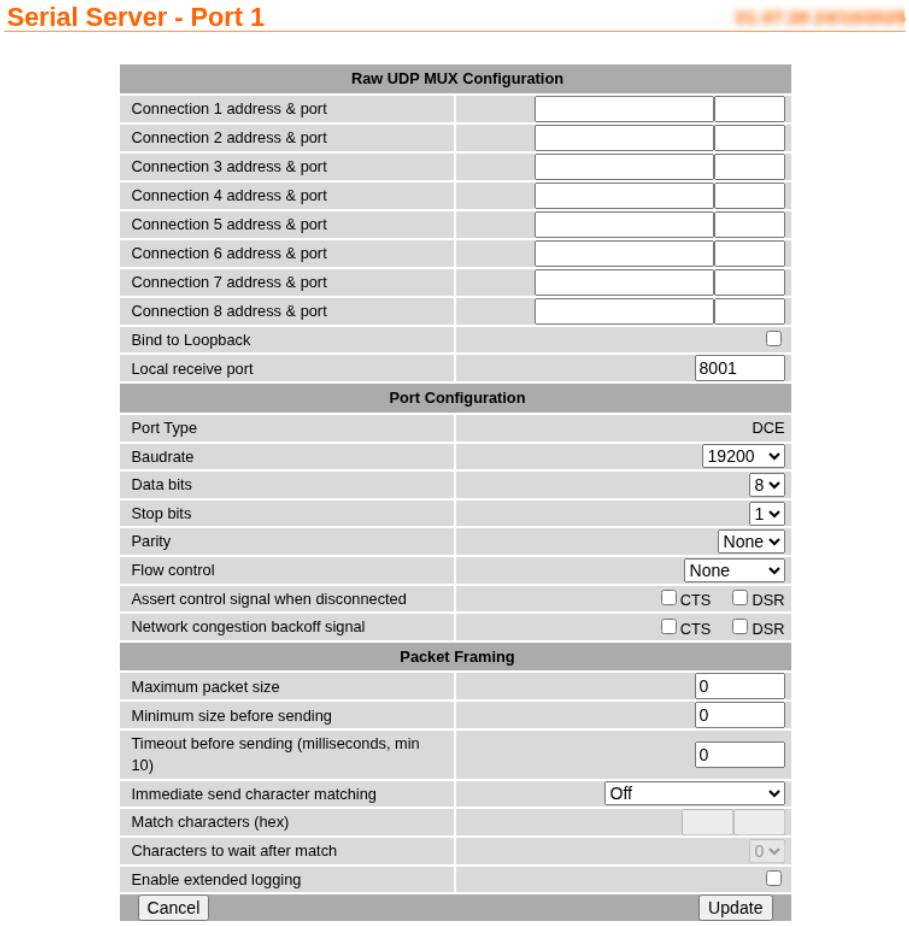


Fig. 12.15: Raw UDP MUX configuration

12.7 Modem Emulator

12.7.1 Description

The serial server provides an AT command interface at the serial port that simulates a traditional dial-up modem. However, instead of dialling out phone calls, the emulator creates TCP network connections. The emulator will also simulate incoming calls if it receives a TCP connection. The function is suited to applications where equipment attached to the serial port expects to see a dial-up modem.

12.7.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the submenu. To enable a port for the Modem Emulator function, select **Modem Emulator** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.16.

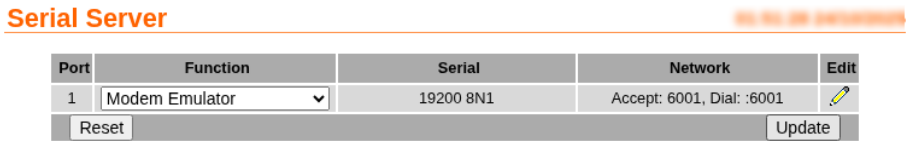


Fig. 12.16: Selecting Modem Emulator function

Port Control

When in modem emulator mode the serial port accepts AT commands. These commands may affect the behaviour of the port. Clicking the Reset Port button will reset the port to the initial state.

12.7.3 Modem Emulator Configuration

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.17, will be displayed.

The following options can be set:

Modem Emulator Configuration

Dial out destination address

This field determines how the emulator will handle dial requests from the serial port (ATDxxxx commands). The dial address may be set to:

Fixed destination

Regardless of the value entered after the ATD command, the emulator will always connect to the host specified in the **Fixed destination address** and **Fixed destination port** fields.

From dial string

The emulator will parse the ATD command to extract the destination address and port number. The examples below show the two different formats that can be used to create a connection to the address 10.10.10.10 and port number 6001.

Dotted

Dial string is ATD 10.10.10.10:6001

Padded

Dial string is ATD 01001001001006001

From phone book

When a dial command is entered, the emulator will look up the modem's phone book and attempt to translate the number to an address and port number.

For more details on the phone book refer to *Phone Book*

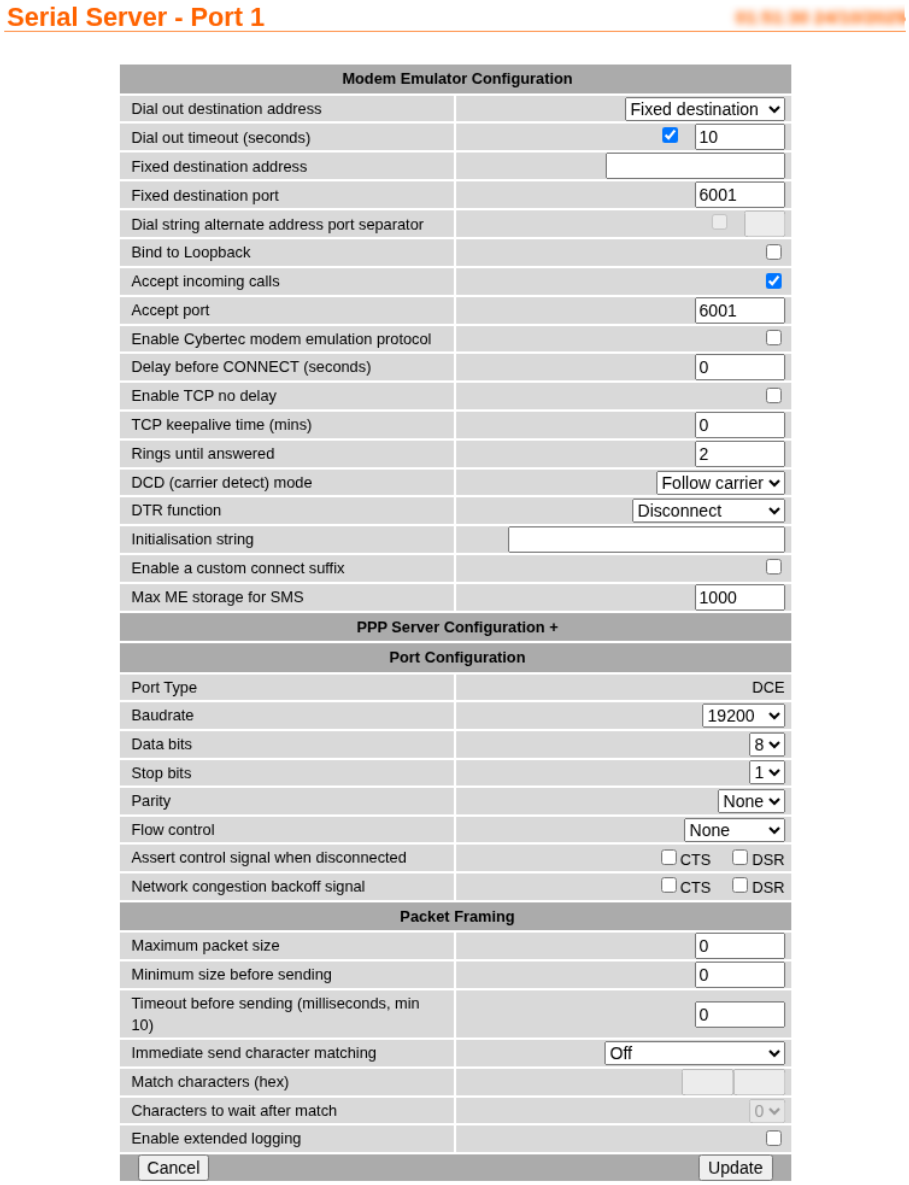


Fig. 12.17: Modem Emulator configuration.

Dial out timeout (seconds)
Check to enable and enter the connection time-out value in seconds.

Fixed destination address
The IP address to connect to if a fixed destination is selected.

Fixed destination port
The IP port to connect to if a fixed destination is selected.

Dial string alternate address port separator
Check to enable and enter a character which separates the IP address from the port number when entered as part of the dial string. The default character is ':'.

Bind to Loopback
Check to bind the service to the loopback interface.

Refer to the *Loopback Interface* section for details on configuring the loopback interface.

Accept incoming calls
Check to enable.

When enabled, the emulator will listen for TCP connections on the port number specified in the **Accept port** field. When a connection is received, the emulator will indicate a ring condition at the serial port. The equipment can then answer the call or wait for the emulator to automatically answer. Once answered, the emulator will indicate the connection is open and data will pass between the remote host and the serial port.

Accept port
This is the TCP port number that the server will listen for connections.

Enable Cybertec modem emulation protocol
Check to enable.

When enabled, the modem emulator will emulate a modem using the Cybertec modem emulation protocol.

Refer to *AT Commands* for details on the Cybertec modem emulation protocol.

Delay before CONNECT (seconds)
Enter a delay in seconds from the time of connection to when the CONNECT string is sent. Default value is 0 or no delay.

Enable TCP no delay
Check to enable TCP no delay.

> **Note**
>
> TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once.
>
> For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reasons that it is not recommended to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

TCP keepalive time (mins)
When set to a value greater than 0, TCP keep-alives will be enabled for connections, with probes sent at the frequency specified (minutes). This may assist in detecting failed connections.

Rings until answered
This field determines the default number of rings the emulator will wait for before automatically answering a call. This is equivalent to setting the ATS0 S-Register in a conventional modem.

DCD (carrier detect) mode
This field determines the default state of the Data Carrier Detect (DCD) handshaking line. The following modes are supported:

Always off
The DCD line will always be inactive.

Always on
Regardless of the online state of the emulator, the DCD line will be active (equivalent to AT&C0).

Follow carrier
The DCD line will be active when the emulator is in the online state (equivalent to AT&C1).

> **Note**
>
> The DCD mode only applies when the port type is DTE.
>
> If the port type is not DTE this setting will be ignored.

DTR function
This field determines the default response of the modem to changes in the Data Terminal Ready (DTR) handshaking line. The following modes are supported:

Ignore
The emulator will ignore changes to the state of DTR (equivalent to AT&D0).

Command mode
If the DTR line transitions from the active to inactive state while the emulator is in online data mode, the emulator will drop to AT command mode (equivalent to AT&D1).

Disconnect
If the DTR line transitions from the active to inactive state while the emulator is in online data mode, the emulator will terminate the current call (equivalent to AT&D2).

> **Note**
>
> The DTR function only applies when the port type is DCE.
>
> If the port type is not DCE this setting will be ignored.

Initialising string
Enter a string which will be sent as part of the initialisation process. Default is no string will be sent.

Enable a custom connect suffix
Check to enable.

When enabled, the emulator will append the string entered in the **Connect suffix** field to the CONNECT string.

Custom connect suffix
Enter a string which will be appended to the CONNECT string. Default is no string will be appended.

Max ME storage for SMS
Set the maximum number of SMS messages that can be stored in the modem emulator memory.

Click the Update button to save and commit the changes.

12.7.4 PPP Server configuration

The modem emulator includes a PPP server which can be enabled if required. To access the PPP Server configuration click the heading, the display will change to include the options shown in Fig. 12.18.

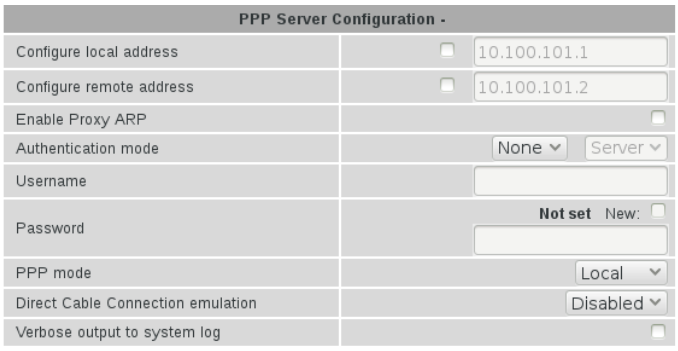


Fig. 12.18: Modem Emulator PPP configuration.

The following options are available:

PPP Server Configuration:

Configure local address
Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Configure remote address
Check to enable and enter an IP address. This is the IP address the modem will allocate to the connected PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the local IP address.

Enable Proxy ARP
Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication mode
This field sets the required level of authentication for remote users connecting to the modem when operating in Server mode or the authentication to use when operating in client mode and connecting to a remote server.

Authentication type

None
No authentication will be required.

PAP
Authentication will be required using the PAP protocol.

CHAP
Authentication will be required using the CHAP protocol.

Mode

Server
Set to PPP server. Receive remote connections.

Client
Set to PPP client. Connect to remote servers.

Username
Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password
Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

PPP mode
Select from:

Local
Ignores the serial port control lines.

Modem
Uses the serial port control lines.

Direct Cable Connection emulation
Direct Cable Connection (DCC), is a feature of Microsoft Windows which allows a computer to transfer data with another computer, using either the serial port of each computer. This option is only available if the PPP mode is set to local. Select from:

Disabled
Disabled Direct Cable Connection.

Host
Act as the host and receive connections from a guest.

Guest
Act as the guest and make a connection to a host.

Verbose output to system log
Check box to enable extended logging information to be written to the log file. This can be useful to assist when first configuring the PPP settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Packet Framing
For information on setting the Packet Framing, refer to *Packet framer settings*.

Click the Update button to save and commit any configuration changes.

12.8 DNP3 IP-Serial Gateway

12.8.1 Description

The DNP3 IP-Serial Gateway carries out translation between DNP3 Serial and DNP3 TCP protocols. This has several advantages:

- DNP3 frames are not fragmented. The translation software identifies and transmits DNP3 link layer frames without fragmentation, ensuring reliable transport of the DNP3 data in a single TCP or UDP packet.
- Server serial port emulation is not required. The SCADA server can communicate with the DNP3 device directly via TCP rather than through serial port emulation software. This reduces the complexity and number of software layers required on the SCADA servers.
- Dual function endpoint. The remote station can return unsolicited messages DNP3 serial data to the SCADA server.

12.8.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the submenu. To enable a port for the DNP3 IP-Serial Gateway function, select **DNP3 IP-Serial Gateway** from

the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.19.

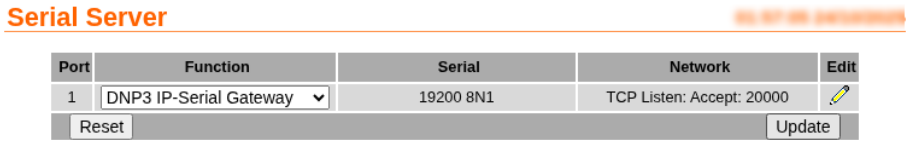


Fig. 12.19: Selecting DNP3 Gateway function

12.8.3 Configuring the port function

Once the port function has been selected, click on the  icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.20, will be displayed.

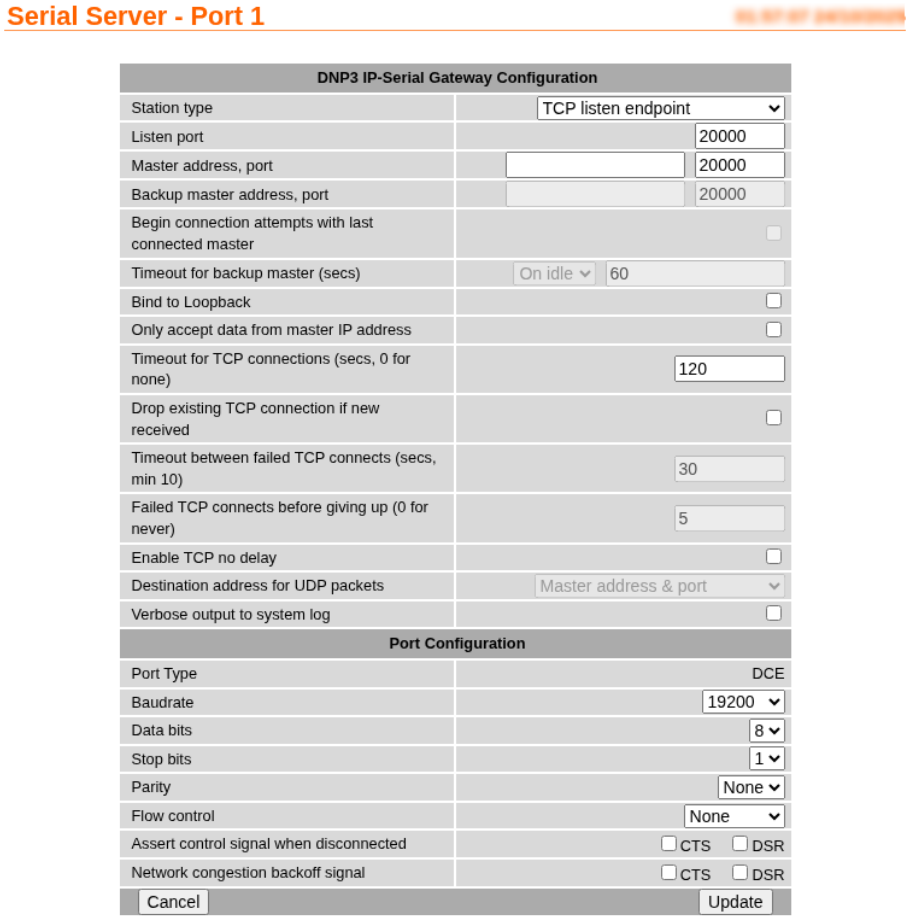


Fig. 12.20: DNP3 Gateway configuration

The following options are available:

DNP3 IP-Serial Gateway Configuration:

Station type

The DNP3 IP-Serial Gateway can be configured to operate in one of the following modes:

TCP listen endpoint

The serial server will listen for TCP connections on the specified port number.

TCP dual endpoint

The serial server will normally listen for TCP connections on the specified port number. If however

a valid DNP packet is received at the serial port and no connection exists, a connection will be established to the specified master address. This is useful if a SCADA master will poll periodically but a facility is required to support unsolicited responses.

TCP redundant dual endpoint
Similar to the TCP dual endpoint option but includes a backup DNP master.

UDP (datagram) endpoint
The serial server will operate in UDP mode, receiving data on the specified port number and transmitting responses to the specified master.

Listen port
For all station types, this determines the TCP/UDP port the serial server will listen for connections (TCP) or data (UDP) on. The value entered should be a valid TCP/UDP port number. The default DNP3 port number is 20000.

Master
DNP3 master address and port number:

address
The IP address of the SCADA master. The address entered should be in IPv4 decimal dotted notation.

port
The TCP/UDP port the serial server will connect to (TCP) or transmit to (UDP). The value entered should be a valid TCP/UDP port number. The default DNP3 port number is 20000.

Backup master
DNP3 backup master address and port number:

address
The IP address of the SCADA master. The address entered should be in IPv4 decimal dotted notation.

port
The TCP/UDP port the serial server will connect to (TCP) or transmit to (UDP). The value entered should be a valid TCP/UDP port number. The default DNP3 port number is 20000.

Begin connection attempts with last connected master
Check to enable. When enabled, the serial server will attempt to connect to the last connected master before attempting to connect to the primary master.

Timeout for backup master (secs)
Specify the time for which to stay connected to the back master before attempting to connect to the primary master. Options:

Disabled
Stay connected to the backup master indefinitely. An attempt to connect with the primary master will only be made if the connection to the backup master is lost.

Fixed
The connection to the backup master will be maintained for the specified time in seconds.

On idle
The connection to the backup master will be maintained until an idle time of the value specified is detected.

Bind to Loopback
Check to bind the service to the loopback interface.

Refer to the *Loopback Interface* section for details on configuring the loopback interface.

Only accept data from master IP address
When set, this field will cause the serial server to only accept data sourced from the address set in the **Master address** field.

Timeout for TCP connections (secs, 0 for none)
For TCP connections only, when this field is set to a value greater than 0, the serial server will close connections that have had no receive activity for longer than specified (seconds).

Drop existing TCP connection if new received
For TCP connections only, if a connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Timeout between failed TCP connects (secs, min 10)
For **TCP dual endpoint** only, if a connection request has failed, the server will wait the amount of time (in seconds) specified in this field before attempting another connection request. While a short time-out may cause the connection to be established more quickly, it may also cause greater network traffic if the remote host is unavailable and repeated attempts fail.

Failed TCP connects before giving up (0 for never)
For **TCP dual endpoint** only, the serial server will attempt to establish a connection for the number of times specified in this field before giving up and waiting for a connection to be accepted.

Enable TCP no delay
Check to enable TCP no delay.

> **Note**
>
> TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once.
>
> For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reasons that it is not recommended to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

Destination address for UDP packets
For **UDP endpoint** only, the serial server can be configured to behave as follows:

Master address and port
Packets transmitted over the network will always be sent to the address specified in the **Master address** and **Master port** fields.

Address and port of last request
Packets transmitted over the network will be sent to the source address of the most recently received packet. If no packets have been received, packets will be transmitted to the address specified in the **Master address** and **Master port** fields.

Verbose output to system log
Check box to enable extended logging information to be written to the log file. This can be useful to assist when first configuring the DNP3 settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

For information on setting the Port configuration, refer to *Serial port settings*.

Click the Update button to save and commit any configuration changes.

12.9 Modbus IP-Serial Gateway

12.9.1 Description

The Modbus IP-Serial Gateway carries out translation between Modbus/TCP and Modbus/RTU or Modbus/ASCII. This means that Modbus serial slaves can be directly attached to the modem's serial ports without any external protocol converters.

12.9.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the Modbus IP-Serial Gateway function, select **Modbus IP-Serial Gateway** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.21.

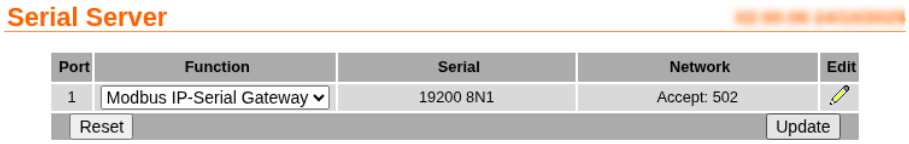


Fig. 12.21: Selecting Modbus Gateway function

12.9.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.22, will be displayed.

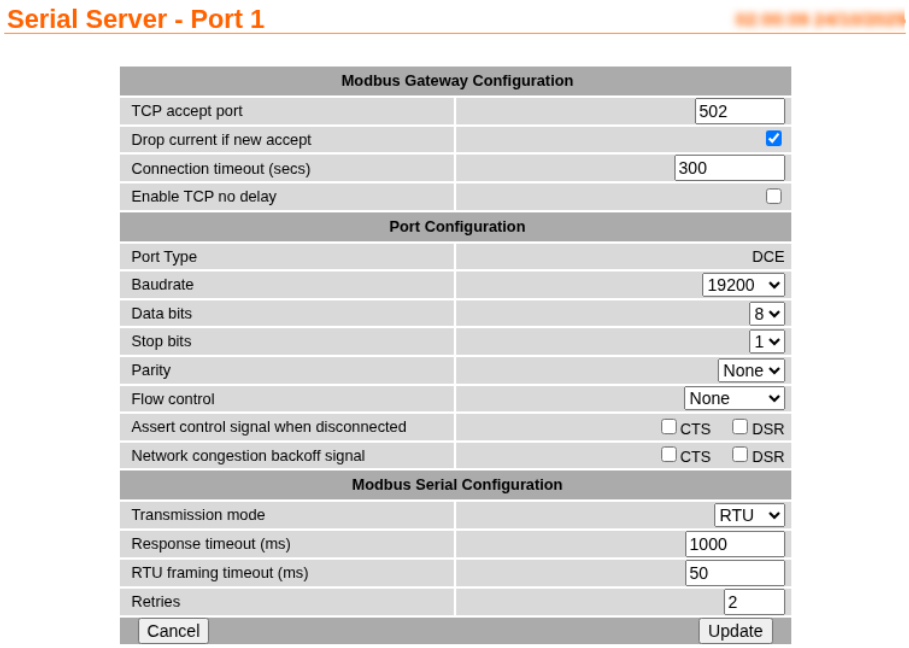


Fig. 12.22: Modbus Gateway configuration

The following options are available for the Modbus Gateway:

Modbus Gateway configuration

TCP accept port

This field determines the TCP port number that the serial server will listen for connections on. The value entered should be a valid TCP port number. The default Modbus/TCP port number is 502.

Drop current if new accept
If a connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Connection timeout (secs)
When this field is set to a value greater than 0, the serial server will close connections that have had no network receive activity for longer than the specified period (in seconds).

Enable TCP no delay
Check to enable TCP no delay.

> **Note**
>
> TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once.
>
> For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reasons that it is not recommended to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Modbus Serial Configuration

Transmission mode
Select RTU or ASCII, based on the Modbus slave equipment attached to the port.

Response timeout (ms)
This is the timeout (in milliseconds) to wait for a response from a serial slave device before retrying the request or returning an error to the Modbus master.

RTU framing timeout (ms)
This is the timeout (in milliseconds) that the serial server will use to determine the boundaries of Modbus/RTU packets received on the serial port.

Retries
Should no valid response be received from a Modbus slave, the value in this field determines the number of times the serial server will re-transmit requests before giving up.

Click the Update button to save and commit any configuration changes.

12.10 Telnet (RFC2217) Server

12.10.1 Description

Telnet server mode is ideal for connecting serial terminal equipment, as a standard Telnet client can be used to connect to the server.

The Telnet server mode also supports the RFC 2217 extensions, which, when used with a remote PC running appropriate serial port redirector software, allow port configuration changes (such as the baud-rate) to be transmitted over the network to the modem. Changes in modem handshaking lines are also transmitted.

12.10.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the submenu. To enable a port for the Telnet Server function, select **Telnet (RFC2217) Server** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.23.

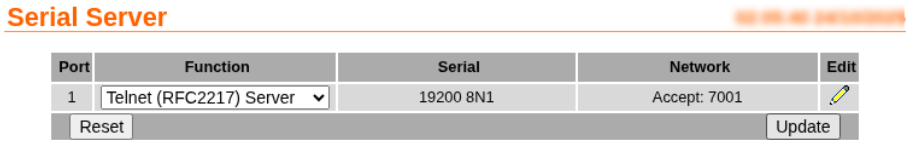


Fig. 12.23: Selecting Telnet Server function

12.10.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.24, will be displayed.

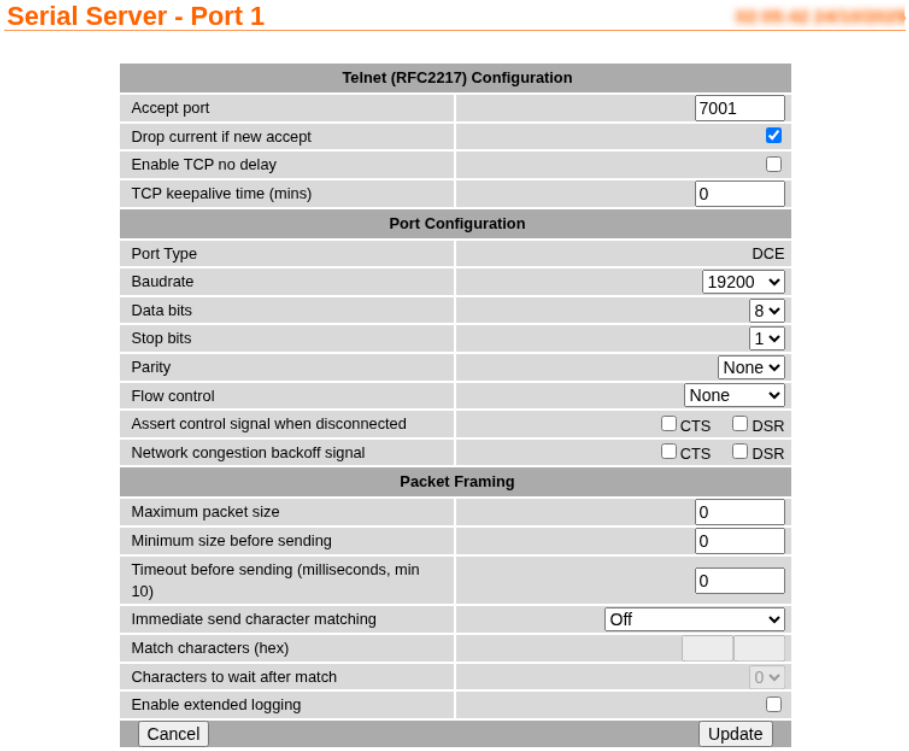


Fig. 12.24: Telnet Server configuration

Telnet (RFC2217) Configuration:

Accept port
: This field determines the TCP port number that the serial server will listen for connections on. The value entered should be a valid TCP port number.

Drop current if new accept
: If a connection is currently active on the serial server, and a new connection request is accepted, this field determines the action that will be taken. If set, the new connection will become the active connection and the existing connection will be closed. If not set, the existing connection will remain active and the newly received connection will be closed.

Enable TCP no delay
Check to enable TCP no delay.

> **Note**
>
> TCP normally uses Nagle's algorithm to combine a number of small outgoing messages, to be sent all at once. Specifically, as long as there is a sent packet for which the sender has not received an acknowledgement, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once.
>
> For serial communications this can introduce delays which can interfere with the operation of serial protocols. Enabling this option will decrease the efficiency of the TCP communications as the number of packets transmitted will increase. It is for these reasons that it is not recommended to enable this option unless the application requires it to be enabled. It could also be that the Raw UDP option may be more suitable.

TCP keepalive time (mins)
When set to a value greater than 0, TCP keep-alives will be enabled for connections, with probes sent at the frequency specified (minutes). This may assist in detecting failed connections.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Packet Framing
For information on setting the Packet Framing, refer to *Packet framer settings*.

Click the Update button to save and commit any configuration changes.

12.11 PPP Server

12.11.1 Description

PPP server is used to allow PPP clients to establish a PPP connection over the serial port.

12.11.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the submenu. To enable a port for the PPP Server function, select **PPP Server** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.25.

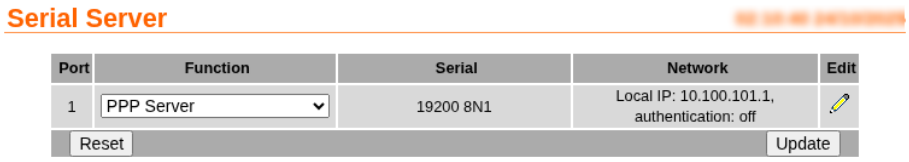


Fig. 12.25: Selecting PPP Server function

12.11.3 Configuring the port function

Once the port function has been selected, click on the icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.26, will be displayed.

PPP Server Configuration:

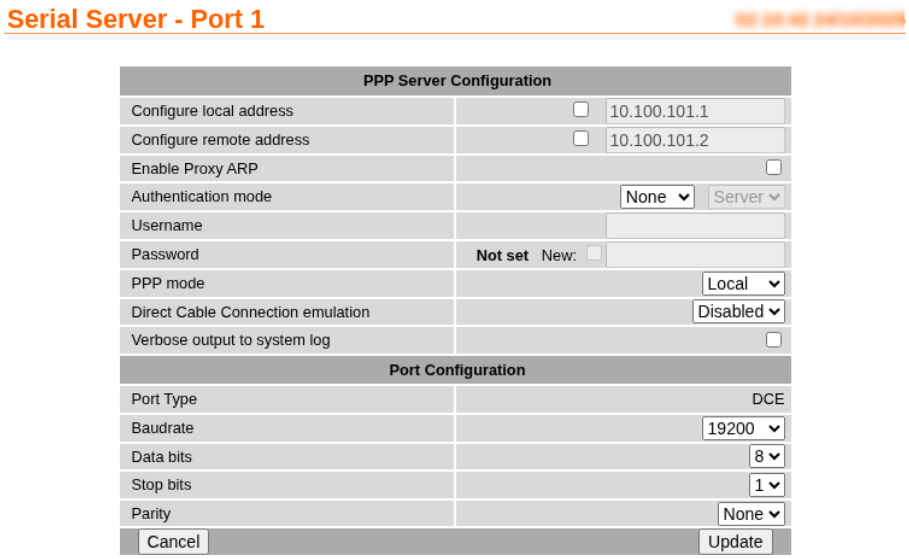


Fig. 12.26: PPP Server configuration

Configure local address
Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Configure remote address
Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the local IP address.

Enable Proxy ARP
Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication mode
This fields sets the required level of authentication for remote users connecting to the modem when operating in Server mode or the authentication to use when operating in client mode and connection to a remote server.

Authentication_type

None
No authentication will be required.

PAP
Authentication will be required using the PAP protocol.

CHAP
Authentication will be required using the CHAP protocol.

Mode

Server
Set to PPP server. Receive remote connections.

Client
Set to PPP client. Connect to remote servers.

Username
Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password
Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

PPP mode
Set the PPP mode. Select from:

Local
Ignores the serial port control lines.

Modem
Uses the serial port control lines.

Direct Cable Connection emulation
Direct Cable Connection (DCC), is a feature of Microsoft Windows which allows a computer to transfer data with another computer, using either the serial port of each computer. This option is only available if the PPP mode is set to local. Select from:

Disabled
Disabled Direct Cable Connection.

Host
Act as the host and receive connections from a guest.

Guest
Act as the guest and make a connection to a host.

Verbose output to system log
Check box to enable extended logging information to be written to the log file. This can be useful to assist when first configuring the PPP settings. It is not recommended to have extended logging enabled in a production system as the log buffer is of limited size and the higher number of logging messages could cause other log messages to be lost.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Click the Update button to save and commit any configuration changes.

12.12 PPP Dial-Out Client

12.12.1 Description

PPP Dial-out Client can be used to establish a PPP connection to a remote PPP server over the serial port. It would typically be used to connect via a dial-up modem connected to the serial port of the unit.

12.12.2 Selecting the port function

The serial server configuration is accessed by selecting **Serial Server** from the main menu and **Port Setup** from the sub-menu. To enable a port for the PPP Dial-Out Client function, select **PPP Dialout Client** from the **Function** column of the appropriate port. Once selected, click **Update** to confirm the change. Once confirmed, the port will display as shown in Fig. 12.27.

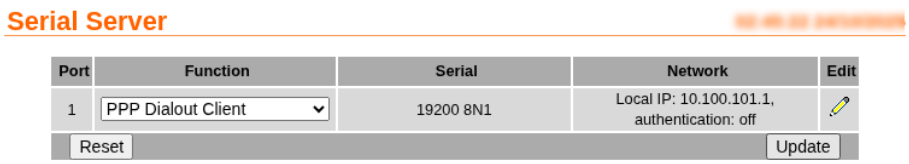


Fig. 12.27: Selecting PPP Dial-Out Client function

12.12.3 Configuring the port function

Once the port function has been selected, click on the  icon, in the **Edit** column to edit settings for the associated port. A page similar to that shown in Fig. 12.28, will be displayed.

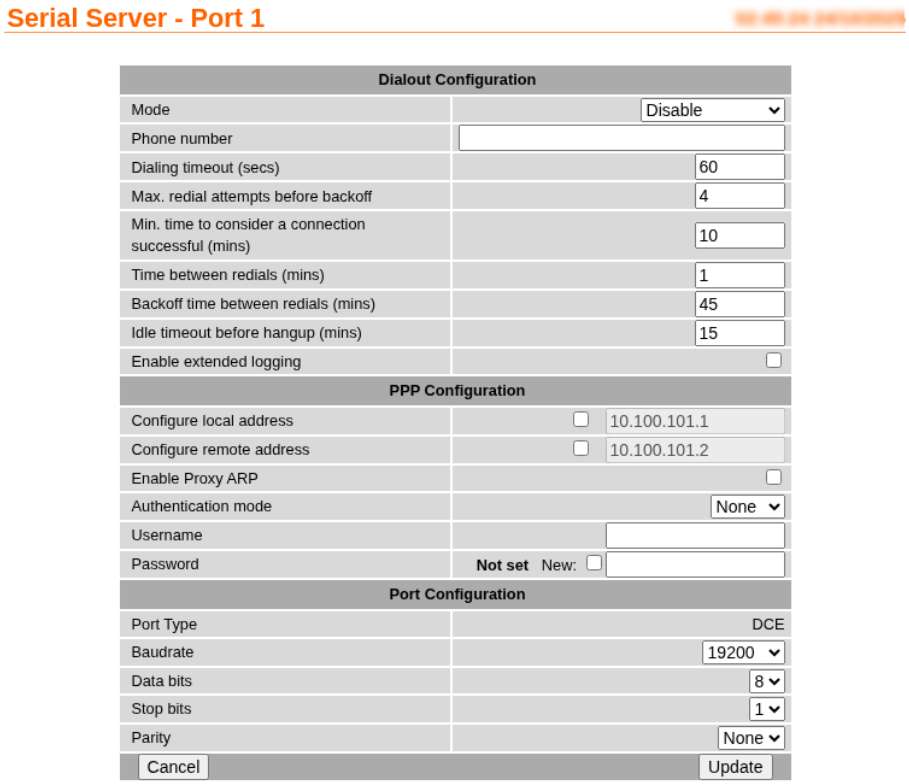


Fig. 12.28: PPP Dial-Out Client configuration

The options available for the configuration of the PPP Dial-Out Client are now described:

Dialout Configuration

Mode
This field sets the operating mode. Available options are:

Disable
Disable dial out.

Manual
The connection is controlled manually by clicking the Connect and Disconnect buttons which are added to the Serial Server page when this mode is selected.

On demand
The connection is made when data is sent to the interface.

Always connect
The connection is permanently established.

Phone number
The number of the remote server to dial.

Dialing timeout (secs)
The time in seconds to wait for a connection after dialling.

Max. redial attempts before backoff
Set the number of failed dialling attempts after which the time between dialling will be increased. This back-off prevents continuously dialling at a fast rate possibly incurring large call costs.

Min. time to consider a connection successful (mins)
The minimum connection time in minutes which is considered a successful connection.

Time between redials (mins)
The time in minutes to wait after a failed dial attempt before redialling.

Backoff time between redials (mins)
The time in minutes to wait to redial after the back-off count has been reached.

Idle timeout before hangup (mins)
The connection is considered idle when no data has been transmitted or received for this time in minutes. Once the idle time is reached the connection will be terminated.

Enable extended logging
If enabled, extended logging information is written to the log. This can assist in diagnosing connection problems.

PPP Configuration

Configure local address
Check to enable and enter an IP address. This is the IP address the modem will have in the PPP connection. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1).

Configure remote address
Check to enable and enter an IP address. This is the IP address the modem will allocate to the connection PPP client. The address entered should be in IPv4 decimal dotted notation (eg. 10.100.100.1) and must be different to the local IP address.

Enable Proxy ARP
Check to enable. Proxy ARP is a technique by which a device on a given network, in this case the modem, answers the ARP queries for a network address that is on a different network, in this case the network of the remote IP address.

Authentication mode
This field sets the required level of authentication for remote users connecting to the modem. Available options are:

None
No authentication will be required.

PAP
Authentication will be required using the PAP protocol.

CHAP
Authentication will be required using the CHAP protocol.

Username
Where **Authentication** is not set to **None**, this is the user-name a remote user will be required to authenticate with.

Password
Where **Authentication** is not set to **None**, this is the password a remote user will be required to authenticate with. To set the password, click the **New** check-box and enter the password in the adjacent field.

Port Configuration
For information on setting the Port configuration, refer to *Serial port settings*.

Click the Update button to save and commit any configuration changes.

12.13 Phone Book

12.13.1 Description

The Phone Book works in conjunction with the Modem Emulator to provide a translation table from traditional phone numbers dialled using the "ATD" command to IP addresses and port numbers. This allows the Modem Emulator to be used as a drop in replacement for a traditional dial-up modem and to create TCP/IP connections rather than making phone calls.

For more information on the Modem Emulator, refer to *Modem Emulator*.

To access the Phone Book configuration, select *Serial Server* → *Phone Book* from the menu. The page will initially have no entries, as shown in Fig. 12.29.

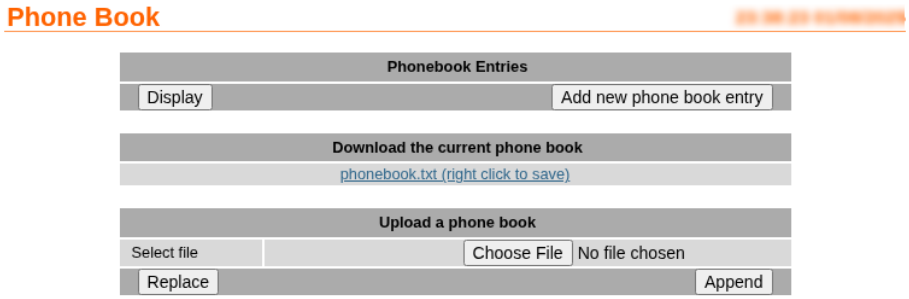


Fig. 12.29: The main Phone Book page

12.13.2 Phonebook Entries

This section shows a summary of the current phone book entries, the Display button displays the complete details of the current entry list in tabular format, and new entries can be added by clicking the Add new phone book entry button.

A phone book entry consists of a dial string and one or more contact addresses. If more than one connection address is entered for a dial string each address is tried in turn until a connection is made.

To add a new phone book entry click the Add new phone book entry button on the main Phone Book page. The phone book entry page will be displayed as shown in Fig. 12.30.

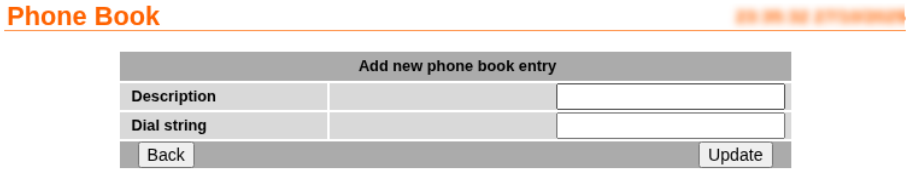


Fig. 12.30: Page for adding Phone Book entry

The following options can be set for each entry:

Description
: A description for the entry.

Dial string
: The dial string which will be matched to received dial strings.

Once the details have been entered click the Update button to save and commit the changes. The page will refresh and now include a table for connection entries, as shown in Fig. 12.31.

To add a connection entry click the Add new connection entry button. The connection entry page will be displayed as shown in Fig. 12.32.

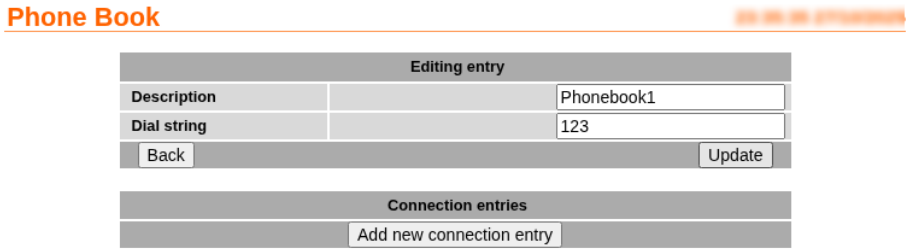


Fig. 12.31: Page for adding Phone Book entry

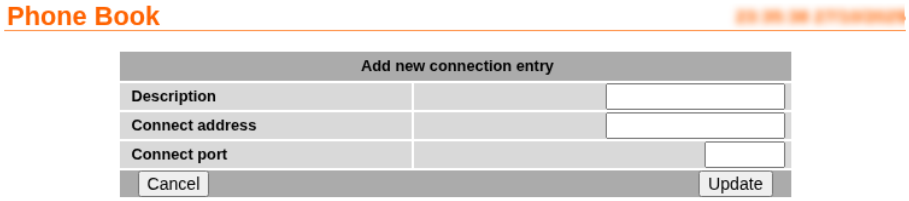


Fig. 12.32: Page for adding connection entry

The following options can be set for each entry:

Description
A description for the entry.

Connect address
This is the IP address the serial server will attempt to connect to.

Connect port
This is the IP port number the serial server will attempt to connect to.

Click the Update button to save and commit the entry. Further entries can be added by repeating the process, each new entry will be associated with the dial string entered at the first step.

After completing the phone book entry click the Back button to return to the main phone book page.

12.13.3 Example of Adding a new phone book entry

In this example a new entry is created that translates dial string 123 to connection address 123.123.123.123:123.

From the main phone book page click the Add new phone book entry button. First the details for the dial string are added as shown in Fig. 12.33.

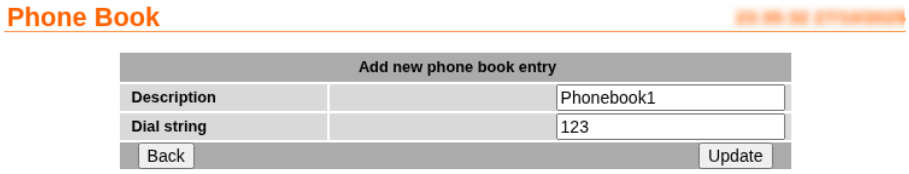


Fig. 12.33: Adding a Phone Book Entry

Click the Update button to save and commit the entry. The page will be updated to include the connection entries table as shown in Fig. 12.34.

Click the Add new connection entry button, now the details for the connection can be added as shown in Fig. 12.35.

Click the Update button to save and commit the connection entry.

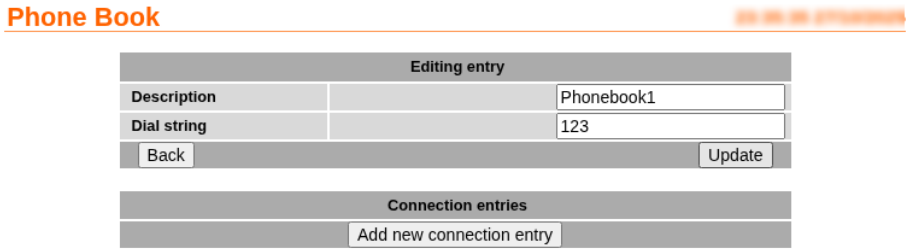


Fig. 12.34: The add phone book entry page with the Connection entries table shown.

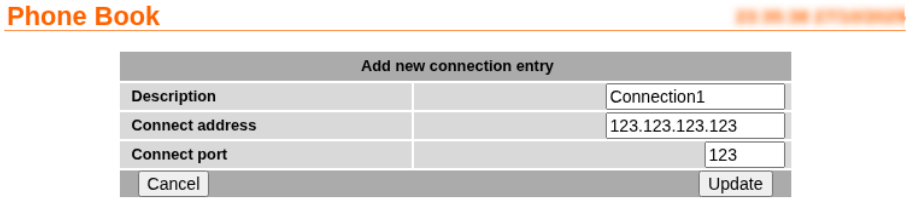


Fig. 12.35: Adding a connection entry with address and port details

The page will return to the phone book entry page with the connection now listed in the Connection entries table, as shown in Fig. 12.36.

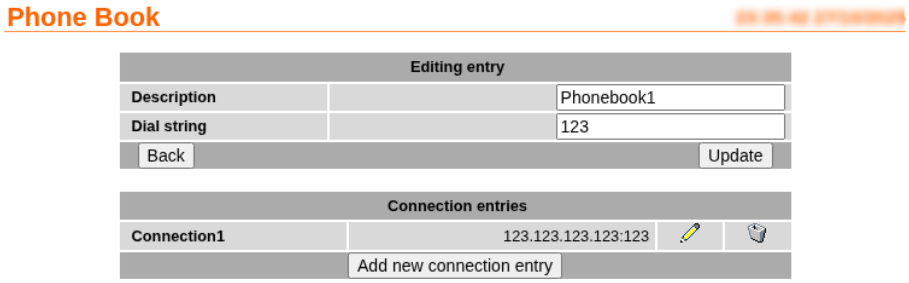


Fig. 12.36: Phone book entry page showing connection

Click the Back button to return to the main Phone Book page.

The page will return to the phone book entry page with the new phone book entry listed in the main table, as shown in Fig. 12.37.

12.13.4 Example of Adding a Second phone book entry

In this example a second entry will be created, called Phonebook2, this entry will translate dial string 234 to two connection addresses, 'Connection1' with address 123.123.123.123:123 and 'Connection2' with address 234.234.234.234:234.

To add a second entry click the Add new phone book entry button. First the details for the dial string are entered as shown in Fig. 12.38.

To commit the new phone book entry to the table, click the Update button.

The add entry page will update to show the connection entries table shown in Fig. 12.39.

Click the Add new connection entry button, now the details for the connection can be added as shown in Fig. 12.40.

Click the Update button to save and commit the connection entry.

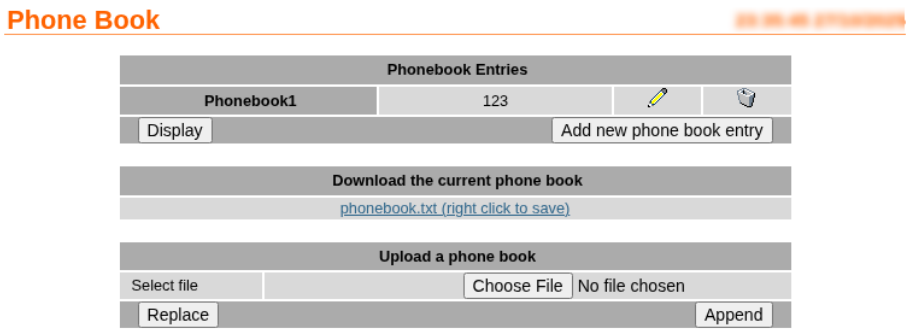


Fig. 12.37: Main Phone Book page with the new phone book entry listed

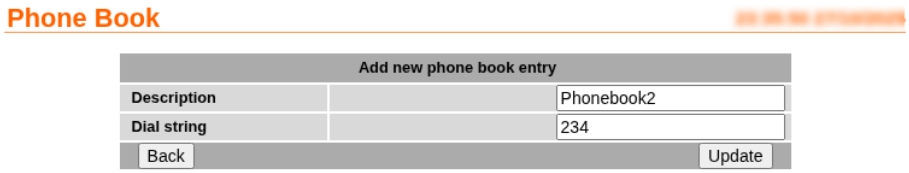


Fig. 12.38: Adding a second phone book entry

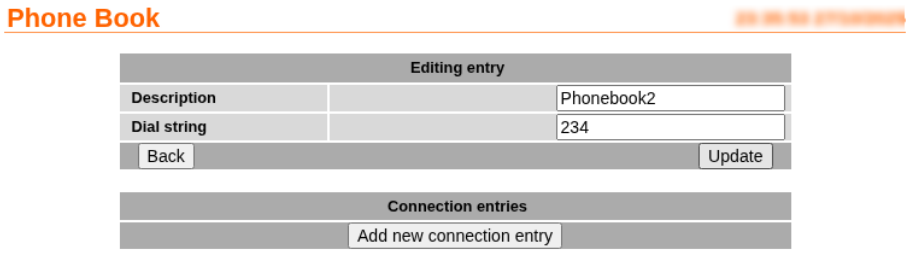


Fig. 12.39: The second phone book entry has been added.

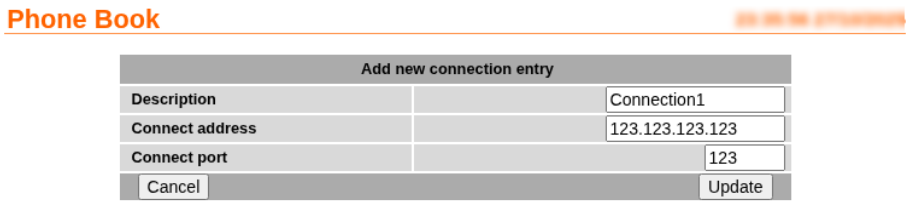


Fig. 12.40: The connection details for the second phone book entry.

The page will return to the phone book entry page with the connection now listed in the Connection entries table, as shown in Fig. 12.41.

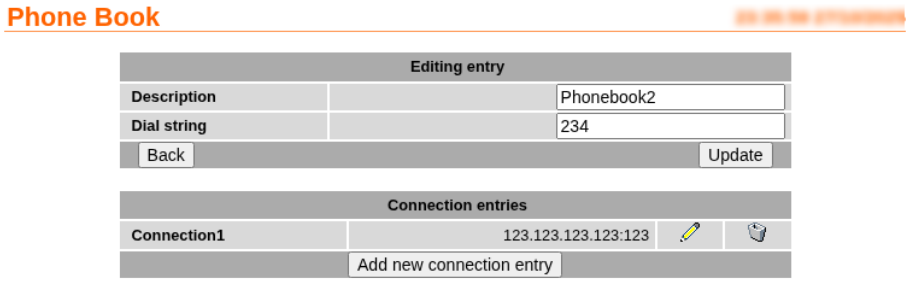


Fig. 12.41: Phone book entry page showing first connection

To add the second connection, again click the Add new connection entry button, the details for the connection can be added as shown in Fig. 12.42.

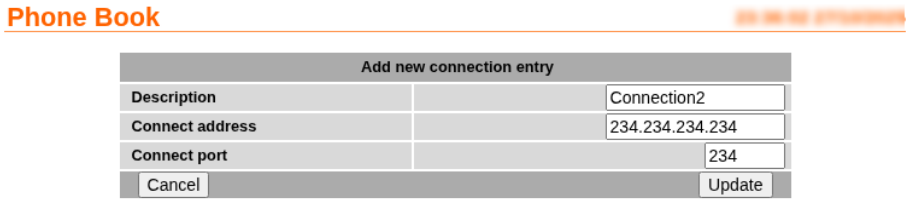


Fig. 12.42: Adding the second connection entry

Click the Update button to save and commit the connection entry.

The page will return to the phone book entry page with both of the connections now listed in the Connection entries table, as shown in Fig. 12.43.

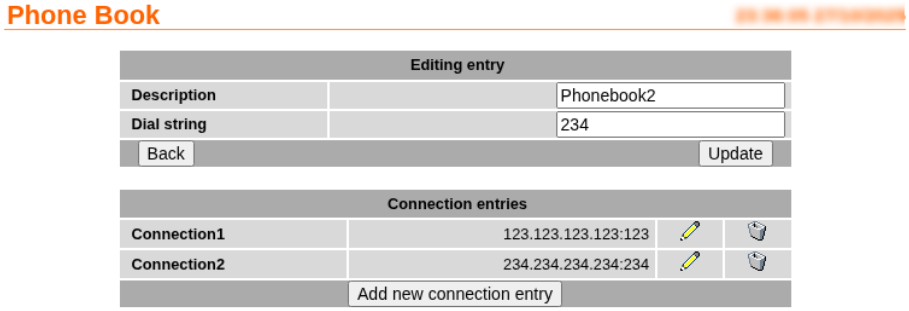


Fig. 12.43: Phone book entry page showing both connections

Click the Back button to return to the main Phone Book page.

The page will return to the phone book entry page with the new phone book entry listed in the main table, as shown in Fig. 12.44.

12.13.5 Display Phone Book Entry Details

The table shown on the main Phone Book page is a summary and does not include the full connection details. To display the list of phone book entries with the connection details for each entry click the Display button. The page shown in Fig. 12.45 is the display page after the two entries described in the examples above have been added.

Click the Back button to return to the main Phone Book page.

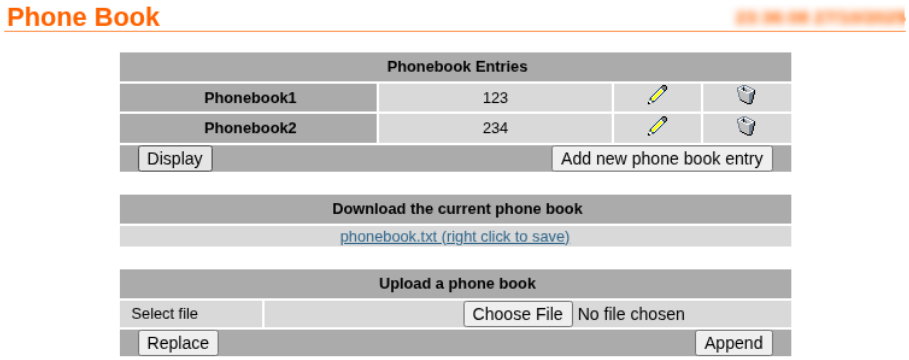


Fig. 12.44: The Phone Book display page with 2 example entries.

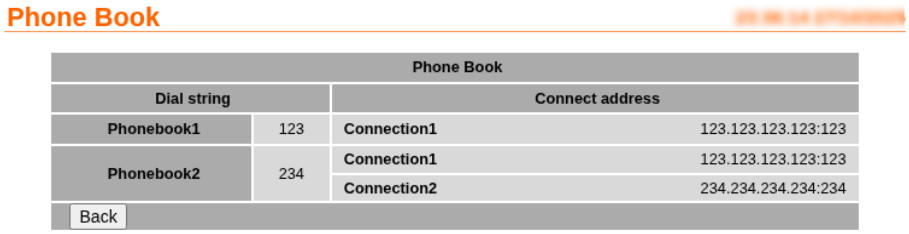


Fig. 12.45: The Phone Book display page with 2 entries.

12.13.6 Editing a phone book entry

A phone book entry can be edited by clicking the icon in the **Edit** column of the entry to be changed. Once clicked, the details of the entry will be displayed in the same table as when creating a new phone book entry.

As an example, to edit the second phone book entry in the table, click the icon in the second row of the table. The editing phone book entry page will be displayed as shown in Fig. 12.46.

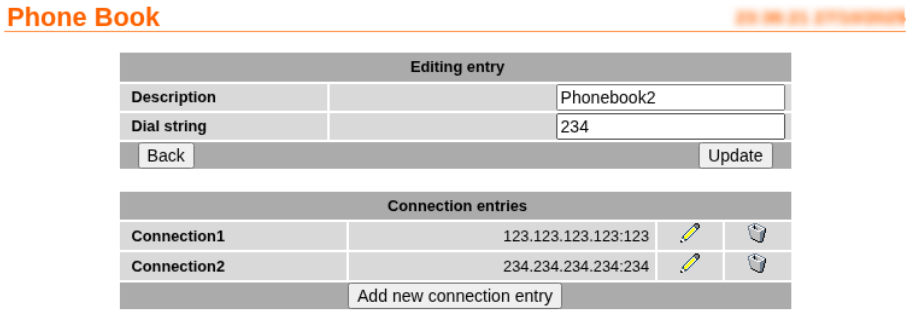


Fig. 12.46: Editing a phone book entry

In this example the dial string will be changed to 235, changes were made as shown in Fig. 12.47.

To save the changes click the Update button or to cancel any changes click the Cancel button.

To return to the main phone book page Click the Back button. The main page will again be displayed as shown in Fig. 12.48, with the changes for entry 2 added to the table.

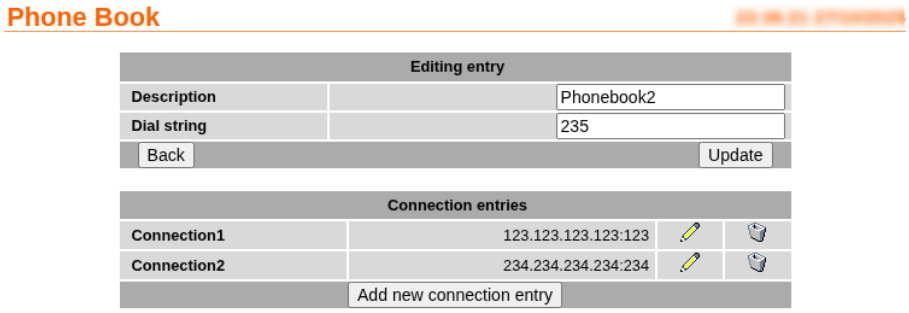


Fig. 12.47: Editing a phone book entry

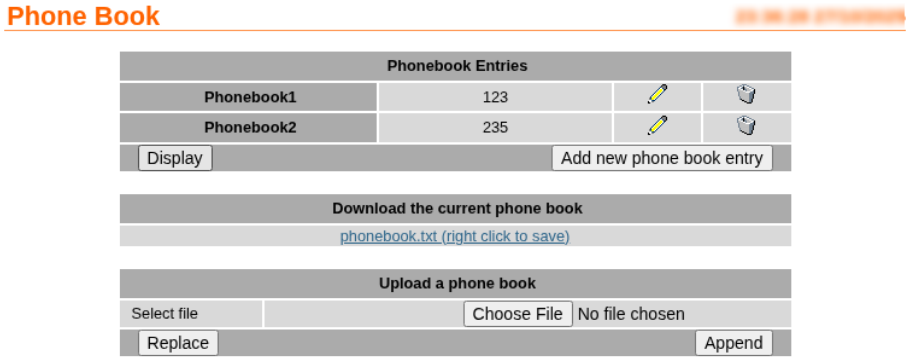


Fig. 12.48: Main phone book page with revised entry

12.13.7 Editing a phone book connection entry

The connection for a phone book entry can be edited by clicking the  icon in the **Edit** column of the connection entry to be changed.

Once clicked, the details of the entry will be displayed in the same table as when creating a new phone book entry.

To edit a connection entry click the  icon in the **Edit** column of the connection entry to be edited.

As an example, the second connection entry 'Connection2' for the 'Phonebook2' entry will be edited to use port 123. To edit the connection entry, first click the  icon in the second row of the table for the entry 'Phonebook2'. Once clicked the details for the phone book entry will be displayed as shown in Fig. 12.49.

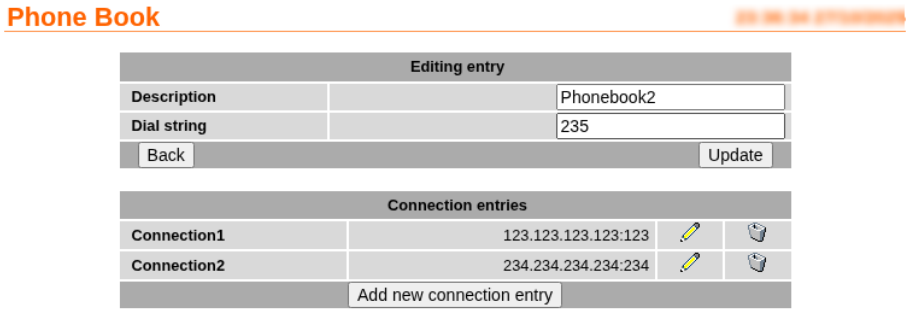


Fig. 12.49: Phone book entry page before editing connection entry

To select the connection entry for editing click the  icon in the second row of the connection entries table. Once clicked the details for the phone book entry will be displayed as shown in Fig. 12.50.

The connections details can now be edited. In this example the port number is changed to 123.

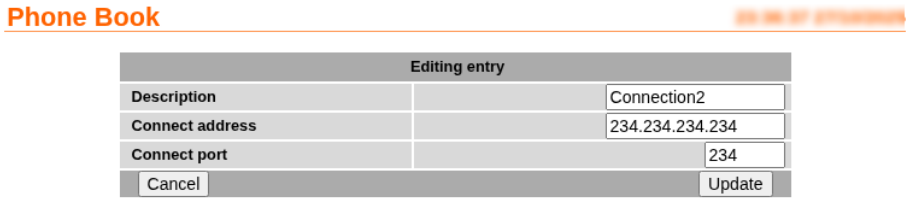


Fig. 12.50: Connection entry editing page before modifications

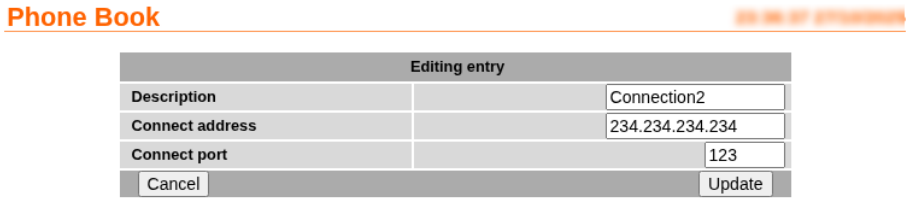


Fig. 12.51: Connection entry editing with modified port number

To save the changes click the Update button or to cancel any changes click the Cancel button.

The phone book entry page will again be displayed as shown in Fig. 12.52, with the changes for connection entry 2 updated in the connection entries table.

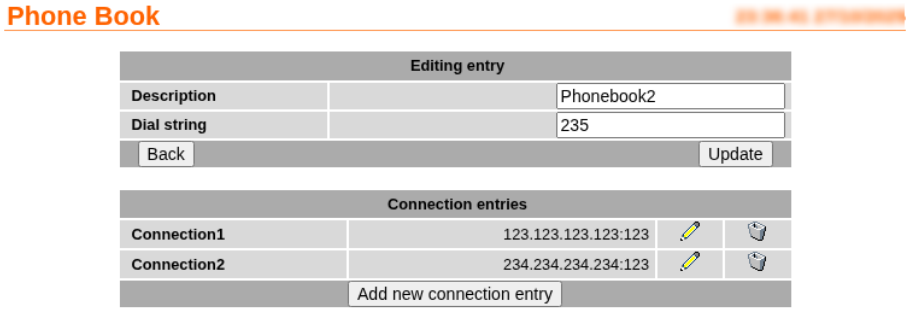


Fig. 12.52: Phone book entry page with updated connection entry

To return to the phone book page click the Back button. The main phone book page will again be displayed as shown in Fig. 12.53.

The table shown is a summary of the phone book entries and so the connection details are not shown. To see the full details of the phone book click the Display button, the full details of the phone book will now be displayed as shown in Fig. 12.54.

To return to the main phone book page click the Back button.

12.13.8 Deleting a phone book connection entry

A phone book connection entry can be deleted by first clicking the edit icon to edit the phone book entry containing the connection entry and clicking the icon in the **Delete** column of the connection entry to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion.

Tip

Deleting of phone book connection details is provided for management of the connection entry details, there is no requirement to delete the connection entries prior to deleting a phone book entry.

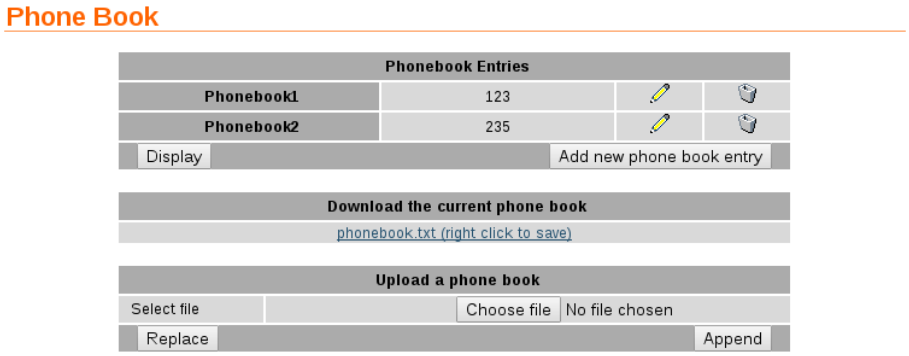


Fig. 12.53: Main phone book page with revised entry

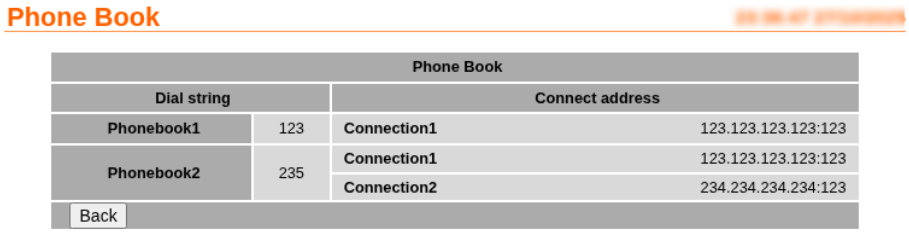


Fig. 12.54: Main phone book page with revised entry

If the entire phone entry is to be deleted refer to the section *Deleting a phone book entry*.

For example, to delete the connection entry 'Connection2' for the phone book entry 'Phonebook2', first click the edit icon for the 'Phonebook2' entry on the main phone book page. The details for the entry will be displayed as shown in Fig. 12.55.

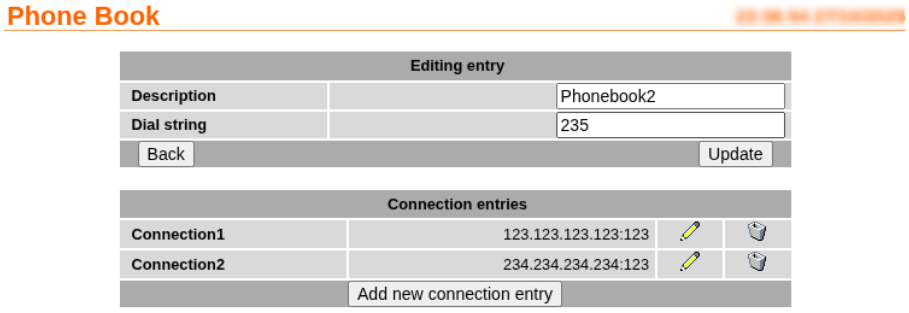


Fig. 12.55: Phone book entry page before deleting connection entry

To delete the connection entry 'Connection2' click the icon in the Delete column of the row labelled 'Connection2'. A warning box will be displayed. Click the OK button to confirm the deletion, as shown in Fig. 12.56.

The connection entry table will be updated with the entry removed, as shown in Fig. 12.57.

To return to the main phone book page click the Back button, as shown in Fig. 12.58 the phone book entries will appear similar to before the deletion because the connection entries are not shown in the summary table.

To display the full updated phone book table click the Display button and the full table will be shown as in Fig. 12.59.

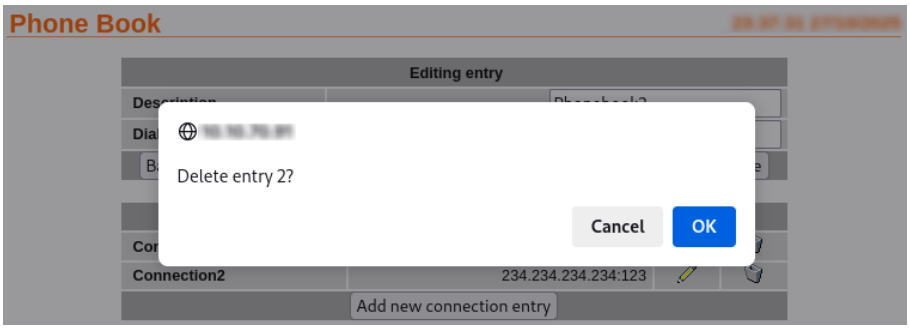


Fig. 12.56: Connection entry deletion confirmation dialog

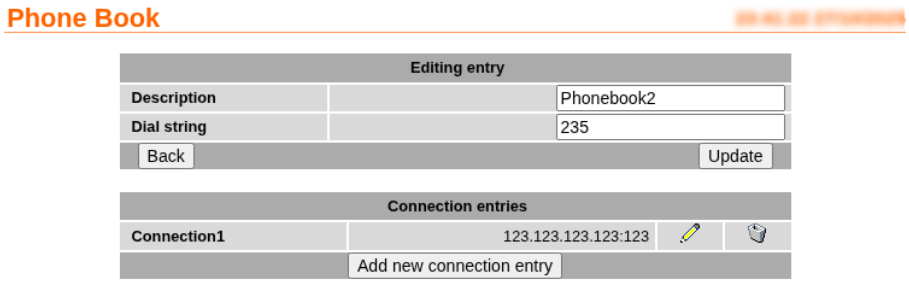


Fig. 12.57: Phone book entry page with connection entry removed

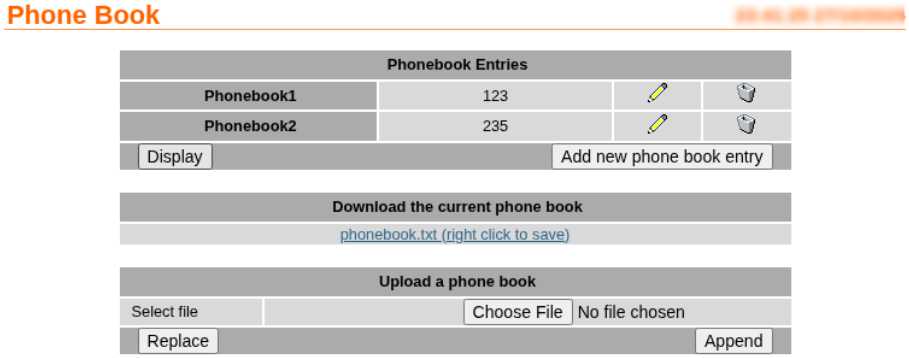


Fig. 12.58: Main phone book page after connection entry deletion

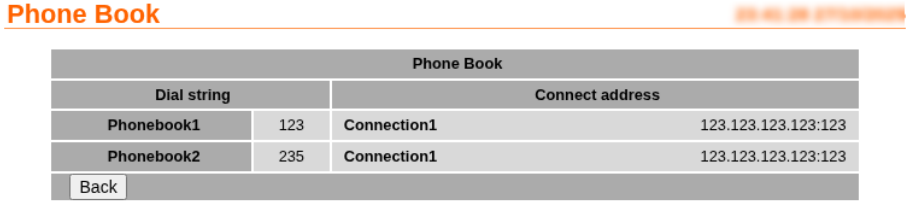


Fig. 12.59: Phone book display page showing entries after connection deletion

12.13.9 Deleting a phone book entry

A phone book entry can be deleted by clicking the icon in the **Delete** column of the entry to be deleted. A warning box will be displayed. Click the OK button to confirm the deletion.

> **Tip**
>
> Deleting a phone book entry will also delete all associated connection entries. There is no requirement to delete the connection entries prior to deleting a phone book entry.

For example, to delete the phone book entry 'Phonebook2' from the table shown in Fig. 12.48, click the icon in row labelled 'Phonebook2'.

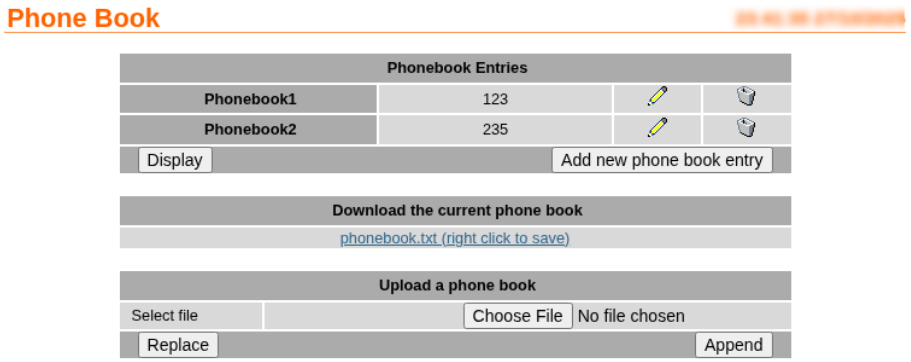


Fig. 12.60: Phone book table before deletion

A warning box will now be displayed as shown in Fig. 12.61. Click the OK button to confirm the deletion.

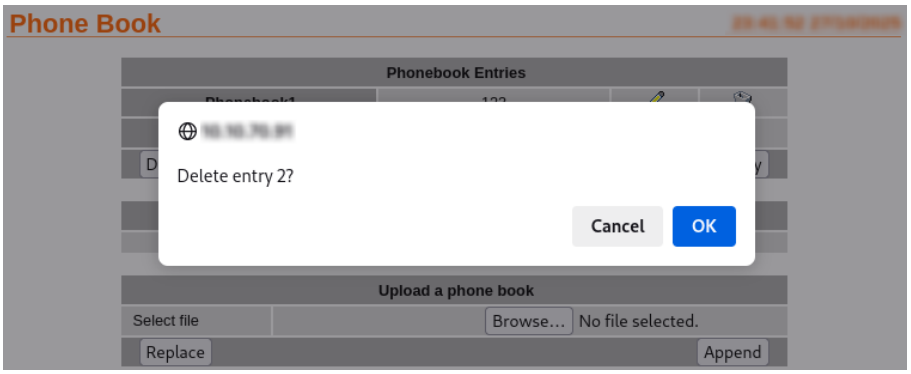


Fig. 12.61: Delete confirmation dialog

The phone book table will be displayed with the entry removed, as shown in Fig. 12.62.

To display the full updated phone table click the Display button, the table will have been updated to that shown in Fig. 12.63.

12.13.10 Exporting the phone book

The current phone book can be exported as a CSV file. The file can be accessed via the link in the section of the page labelled **"Download the current phone book"**. Clicking the link will display the file as a text file. To save the file right click the link and select 'Save as…'.

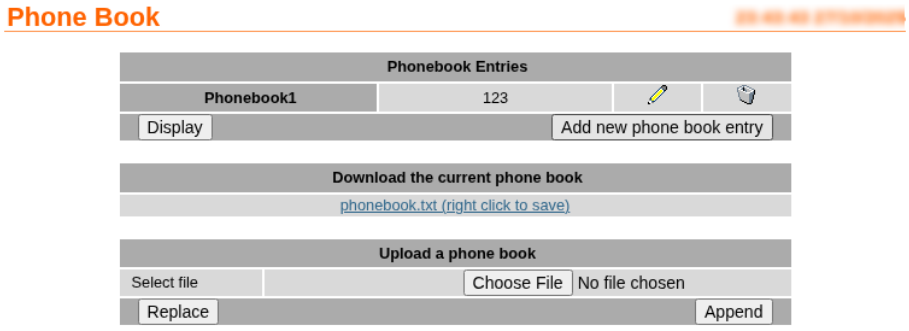


Fig. 12.62: Phone book table after deletion of entry

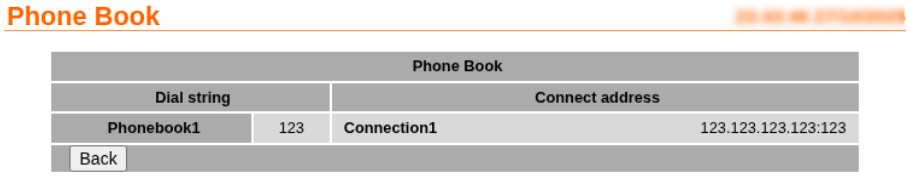


Fig. 12.63: Phone book table after deletion of entry

12.13.11 Importing phone book entries

A CSV file containing phone book entries can be imported. The imported file can either replace the current phone book or be appended to it. To import a file first click the Browse button in the Select file row of the table under the section titled **"Upload a phone book"**, then select the file.

The file name will now be displayed next to the Choose file button. To load the file click either the Replace button to replace all entries in the current phone book with those contained in the file or click the Append button to add the entries in the file to the current phone book.

12.13.12 Phone book CSV file format

The first line of the CSV file contains the column names:

```
"Dial String", "Connect Address", "Connect Port", "Description"
```

The details for the column names are:

Dial String
: The dial string

Connect Address
: The connection IP address

Connect Port
: The connection port number

Description
: The description or label for the entry.

There are 2 types of entries in the file: a dial entry and a connection entry.

Fig. 12.64: The download section of the phone book page.

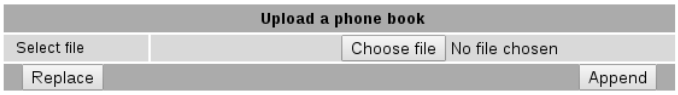


Fig. 12.65: The upload section of the phone book page.

The dial entry contains only a dial string and a description; the other fields are left blank.

An example of a dial entry is:

```
"123", "", "", "Phonebook1"
```

A connection entry has values for each field.

An example connection entry is:

```
"123", "123.123.123.123", "123", "Connection1"
```

For this example the complete listing is:

```
"Dial String", "Connect Address", "Connect Port", "Description"
"123", "", "", "Phonebook1"
"123", "123.123.123.123", "123", "Connection1"
```

12.13.13 Example of importing a phone book

In this example a new phone book entry with a number of connection entries will be added to the phone book. The dial string for the new entry will be labelled 'Phonebook2' for number "456" and it will have associated with it 10 connection entries.

The first step is to create a CSV file for the entries, as shown:

```
"Dial String", "Connect Address", "Connect Port", "Description"
"456", "", "", "Phonebook2"
"456", "123.123.123.120", "123", "Connection0"
"456", "123.123.123.121", "123", "Connection1"
"456", "123.123.123.122", "123", "Connection2"
"456", "123.123.123.123", "123", "Connection3"
"456", "123.123.123.124", "123", "Connection4"
"456", "123.123.123.125", "123", "Connection5"
"456", "123.123.123.126", "123", "Connection6"
"456", "123.123.123.127", "123", "Connection7"
"456", "123.123.123.128", "123", "Connection8"
"456", "123.123.123.123", "123", "Connection9"
```

The file was saved as 'phonebook-Test1.txt'.

The next step is to upload the file, from the phone book page, as shown in Fig. 12.66, click the Browse button in the **'Upload a phone book'** table, and select the file.

Once selected the file name of the file to be uploaded will be shown next to the Choose file button, as shown in Fig. 12.67.

To upload the file click the Append button, the file will be uploaded and the page will update to show the new dial entry for 'Phonebook2', as shown in Fig. 12.68.

To display the full details of the updated phone table click the Display button, the table will have been updated to that shown in Fig. 12.69.

To return to the main phone book page click the Back button.

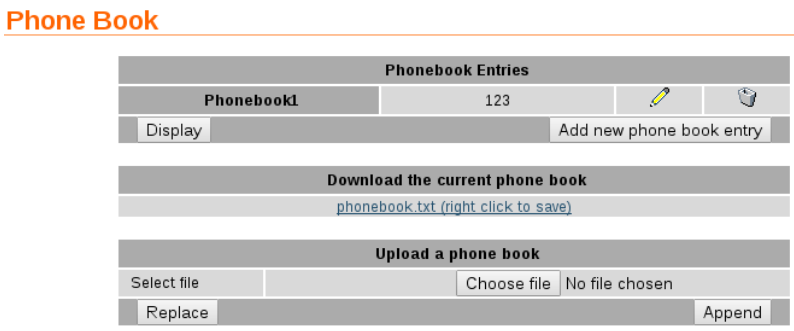


Fig. 12.66: Upload a phone book CSV file.

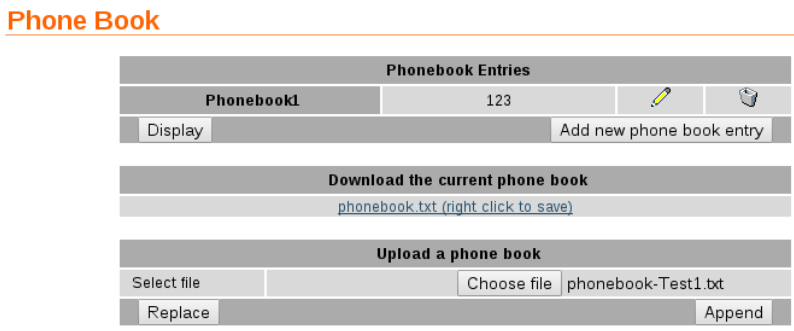


Fig. 12.67: File to be uploaded has been selected.

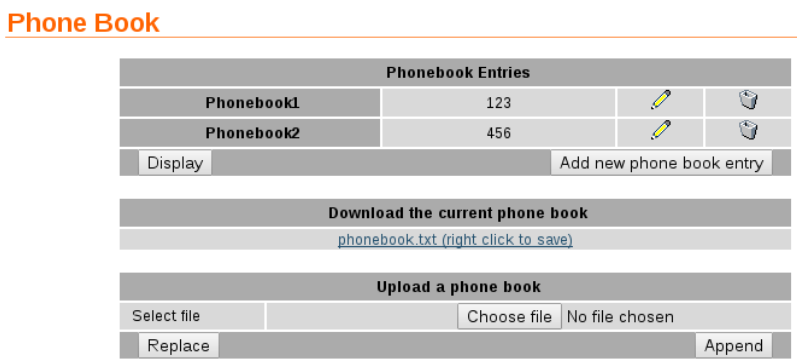


Fig. 12.68: Phone book table with new entry shown.

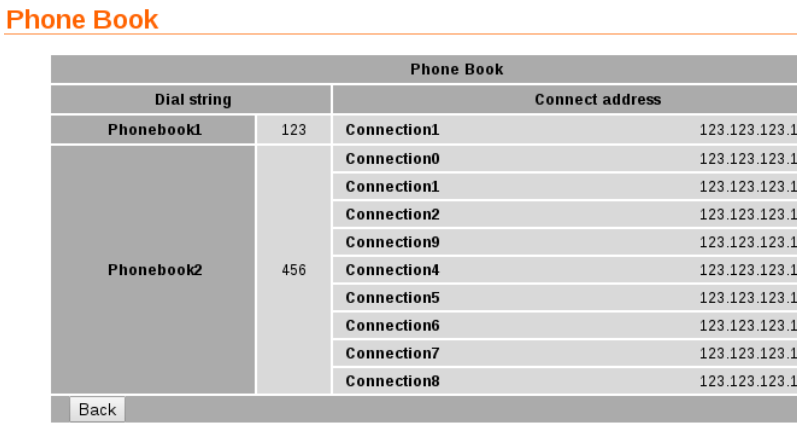


Fig. 12.69: Phone book table with new entries added.

CHAPTER

THIRTEEN

MANAGEMENT

The Management section is used to configure the management and system reporting options for services including events, SNMP, DNP3, SMS and email.

The main management page is accessed by clicking the *Management* tab on the main menu, a page similar to that shown in Fig. 13.1 will be displayed. The number and type of events listed will depend on the model.

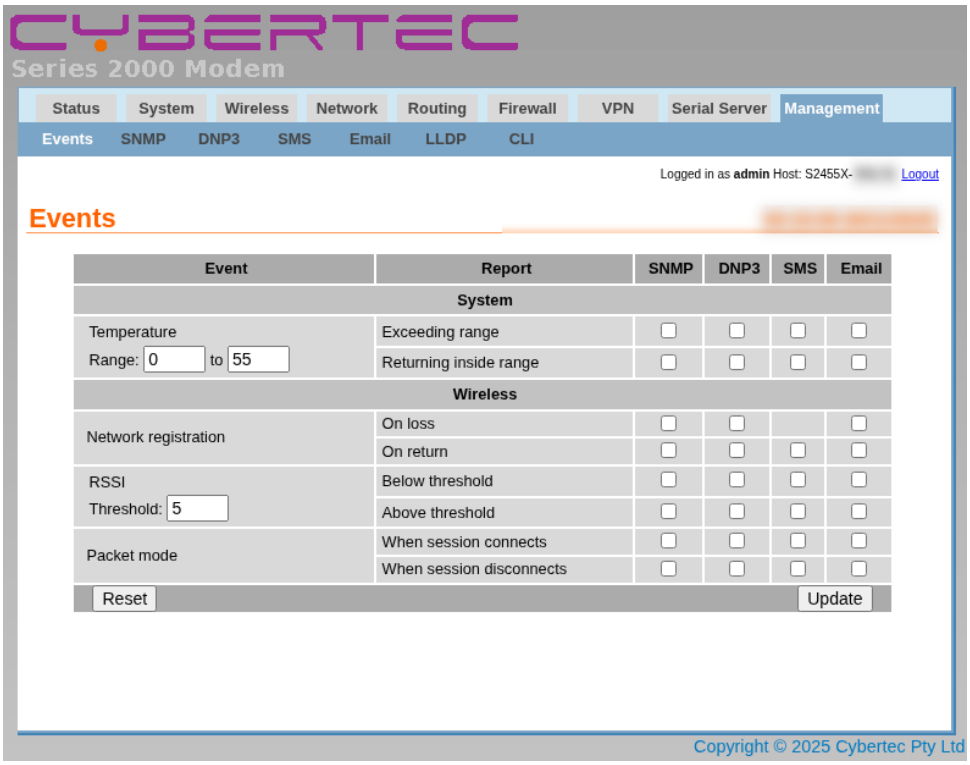


Fig. 13.1: Main management page.

13.1 Events

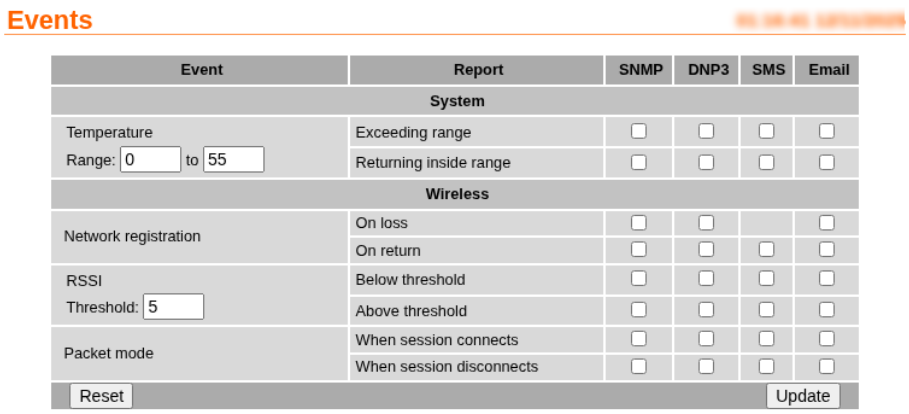
The Events page is selected by clicking *Management* → *Events*. The Events Management page is shown in Fig. 13.2.

For models with GPIO the Events Management page is shown in Fig. 13.3.

13.2 Event Types

The events which may generate triggers are listed in the first column of Events table. The events are as follows:

Temperature
: The nominal operating range may be specified. Events may be generated:

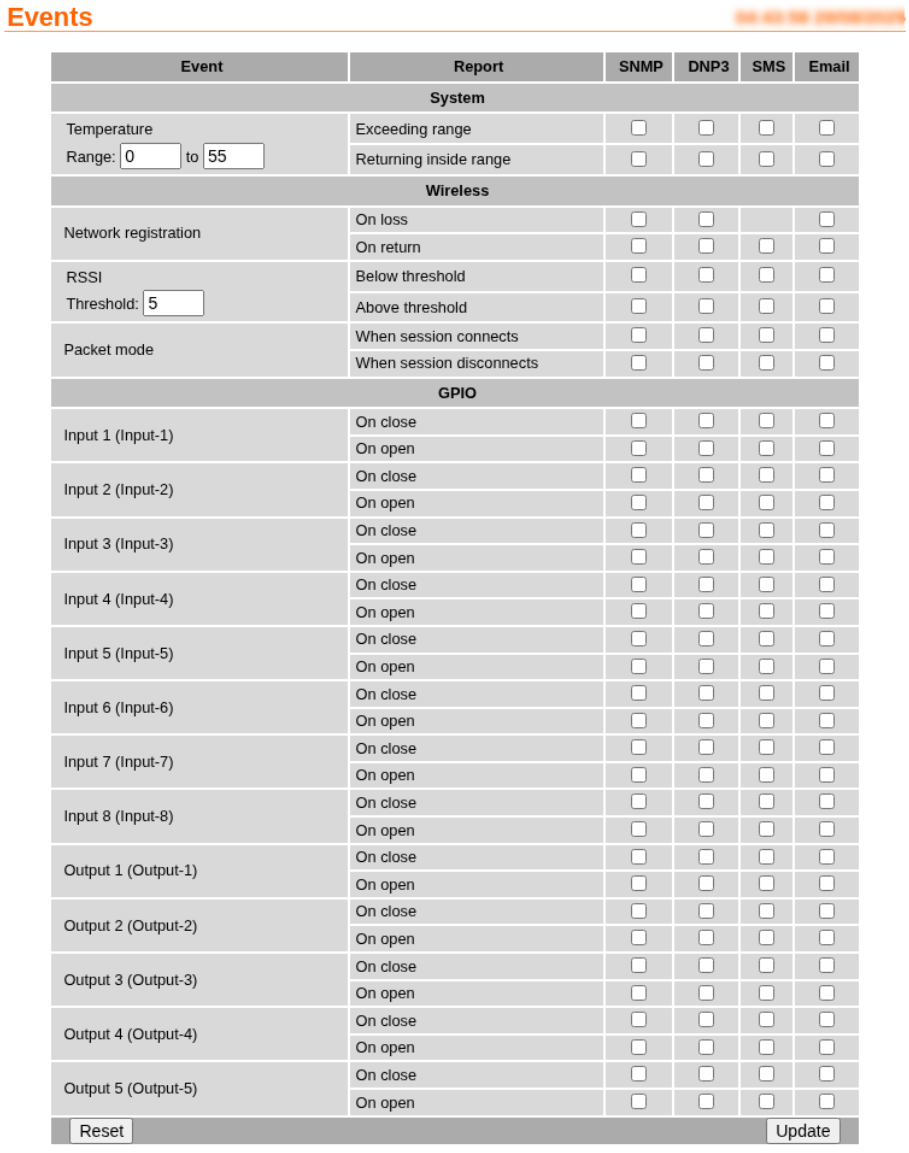


Events

Event	Report	SNMP	DNP3	SMS	Email
System					
Temperature Range: 0 to 55	Exceeding range	☐	☐	☐	☐
	Returning inside range	☐	☐	☐	☐
Wireless					
Network registration	On loss	☐	☐		☐
	On return	☐	☐	☐	☐
RSSI Threshold: 5	Below threshold	☐	☐	☐	☐
	Above threshold	☐	☐	☐	☐
Packet mode	When session connects	☐	☐	☐	☐
	When session disconnects	☐	☐	☐	☐

Reset Update

Fig. 13.2: Management events



Events

Event	Report	SNMP	DNP3	SMS	Email
System					
Temperature Range: 0 to 55	Exceeding range	☐	☐	☐	☐
	Returning inside range	☐	☐	☐	☐
Wireless					
Network registration	On loss	☐	☐		☐
	On return	☐	☐	☐	☐
RSSI Threshold: 5	Below threshold	☐	☐	☐	☐
	Above threshold	☐	☐	☐	☐
Packet mode	When session connects	☐	☐	☐	☐
	When session disconnects	☐	☐	☐	☐
GPIO					
Input 1 (Input-1)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 2 (Input-2)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 3 (Input-3)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 4 (Input-4)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 5 (Input-5)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 6 (Input-6)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 7 (Input-7)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Input 8 (Input-8)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 1 (Output-1)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 2 (Output-2)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 3 (Output-3)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 4 (Output-4)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐
Output 5 (Output-5)	On close	☐	☐	☐	☐
	On open	☐	☐	☐	☐

Reset Update

Fig. 13.3: Events Management with GPIO.

Exceeding range
Triggered when the temperature is outside the nominal range. That is lower than the low temperature to higher than the high temperature as set in the range.

Returning inside range
Triggered when the temperature returns within the nominal range limits.

> **Note**
>
> The current operating temperature is reported on the *Status→Alarms* page. Refer to Section *Alarms* for details.

Network registration
The network registration status. Events may be generated:

On loss
Triggered when the network registration moves from the connected state to the disconnected state.

> **Note**
>
> This event cannot trigger an SMS as it will not be possible to send an SMS without network registration.

On return
Triggered when network registration is established.

RSSI
A threshold may be set for the Receive Signal Strength Indicator (RSSI). Events may be generated:

Threshold
Specify the trigger threshold. Minimum 0, maximum 30

Below threshold
Triggered when RSSI falls below the threshold.

Above threshold
Triggered when RSSI raises above the threshold.

Packet mode
The packet mode status. Event may be generated:

When session connects
Triggered when a packet mode session connects.

When session disconnects
Triggered when a packet mode session disconnects.

Circuit switched mode

> **Note**
>
> Circuit Switched Data mode is not supported on all models.

> **Warning**
>
> Circuit Switched Data mode is generally no longer supported by network operators and the functionality will be removed in a future firmware version.

The Circuit Switched Data (CSD) mode status. Events may be generated:

When online
When CSD connects. This will trigger for both incoming and outgoing connections.

When offline
When CSD disconnects.

> **Note**
>
> The current state of the wireless connection can be found on the *Status→Wireless* page. Refer to Section *Wireless Interface Status* for details.

GPIO
The General Purpose Inputs and Outputs. These events are only available for the models with GPIO. The following events may be generated:

Input n (Input-Name-n)
GPIO Input n, the label associated with the input will be shown enclosed by brackets, where n represent the number of the input.

For example "(Input 1 label").

On close
Triggered when the input transitions from the open to the closed state.

On open
Triggered when the input transitions from the closed to the open state.

Output n (Output-Name-n)
GPIO Output n, the label associated with the input will be shown enclosed by brackets, where n represents the number of the output.

For example "(Output 1 label").

On close
Triggered when the output transitions from the open to the closed state.

On open
Triggered when the output transitions from the closed to the open state.

13.3 Trigger Types

When an event condition is met it may generate a trigger which is any of:

None
The trigger does not generate any message.

SNMP
An SNMP trap is generated.

DNP3
A DNP3 exception is generated.

SMS
An SMS is generated.

Email
An email is generated.

To select a trigger for an event check the check box for the event row corresponding to the trigger type column. For example to enable SNMP traps for Network Registration loss and return check the two check-boxes in the Network registration row, under the SNMP column. This is illustrated in Fig. 13.4 with the Network Registration loss and return selected for SNMP.

Click the Update button to save and commit changes.

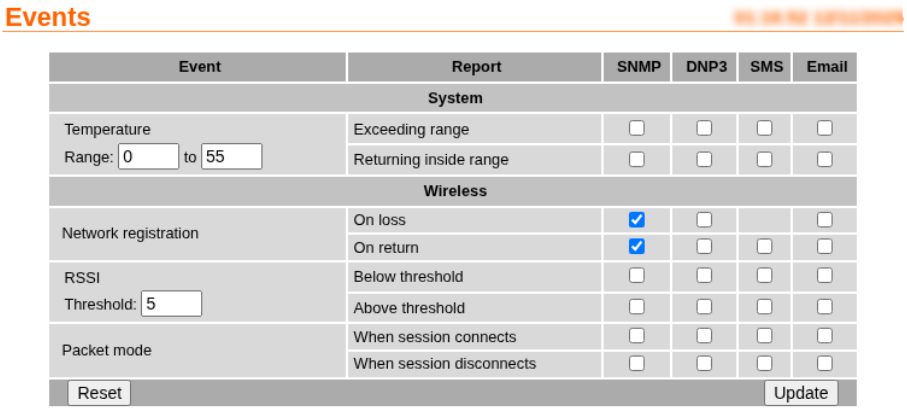


Fig. 13.4: Enabling SNMP traps for the Network Registration events.

13.4 SNMP

The Simple Network Management Protocol (SNMP) can be used for network management of the unit. The current connection status and RF signal level are examples of status variables accessible through SNMP. The custom MIB file for the modem is available for download from the Cybertec

website.

The SNMP configuration options are accessed by selecting *Management→SNMP*. The SNMP configuration page is shown in Fig. 13.5.

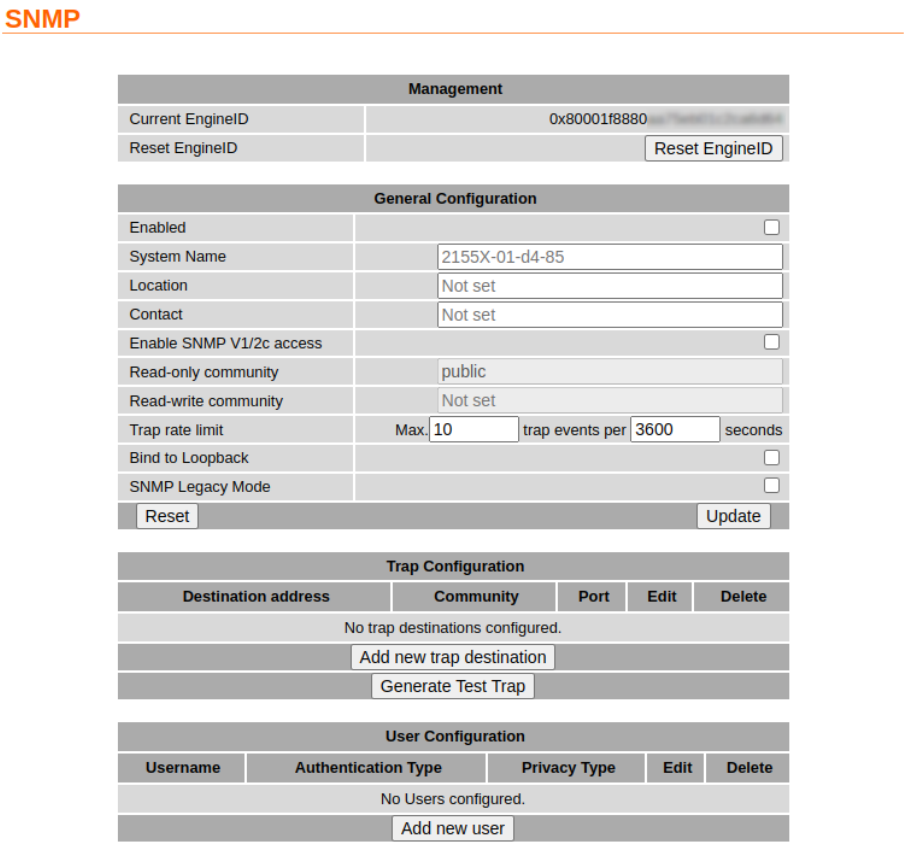


Fig. 13.5: The SNMP configuration page

13.4.1 Management

This section indicates the current SNMP EngineID allows it to be reset.

An SNMP Engine ID is assigned to SNMP Agents and SNMP Management applications which communicate using SNMPv3. The Engine ID is required to be unique across the set of communicating SNMPv3 Agents and Managers.

To reset the SNMP Engine ID click the Reset EngineID button.

> **Warning**
>
> Resetting the SNMP Engine ID will invalidate and delete all user accounts.

A warning message will be shown to proceed click the Ok button and a new EngineID will be generated.

To avoid generating a new EngineID Click the Cancel button.

13.4.2 General Configuration

The general configuration options are described below:

Enabled
Check to enable SNMP.

System Name
The SNMP system name. The default is the host name of the unit.

Location
The location reported in the standard SNMP Location field.

Contact
The contact name reported in the standard SNMP Contact field.

Enable SNMP V1/2c Access
Check to enable SNMP V1 and V2c access. The following fields will then be accessible:

Read-only community
The community string expected for read-only access.

Read-write community
The community string expected for read-write access.

Trap rate limit
Specify the maximum traps over a time period. This can be used to prevent an event trigger which changes more frequently than expected from generating a large number of traps. The timer starts at the time the first trap is sent and resets once the number of seconds configured has elapsed. Format Max. <number> trap events per <time> seconds. Where:

<Number>
Is the maximum number of trap events for the time period; and

<time>
Is the time period in seconds.

Bind to Loopback
Check to to bind SNMP to the Loopback address.

SNMP Legacy Mode
Added in version V1.9.4.0.

Check to enable SNMP legacy mode.

Changes were made to the interface names within the SNMP MIB. Check the SNMP legacy mode to continue to use the original naming.

Click the button Update to save and commit changes. Click the Reset button to cancel the changes and revert to the saved settings.

13.4.3 Trap Configuration

SNMP uses messages called traps to report alerts or asynchronous errors to an SNMP master. Traps can be generated on events such as the RF signal level dropping below a threshold.

The **Trap Configuration** table is used to specify the details of the SNMP master to which SNMP traps will be sent.

To add a new entry click the Add new trap destination button, a page similar to that shown in Fig. 13.6 will appear.

Fig. 13.6: The SNMP trap configuration page.

The following fields can be set:

Destination address
The IP address of the SNMP master.

Community
The community string to send with traps.

Port
The IP port of the SNMP master.

Once the details have been entered, click the Update button to save the new trap destination.

Test traps can be generated by clicking the Generate Test Trap button. This will generate a test trap which will be sent using the details provided when traps were configured.

13.4.4 Example of Adding an SNMP Trap

To add a new entry click the Add new trap destination button, a page similar to that shown in Fig. 13.7 will appear. Add the details for the trap as shown, then click Update the button to save the changes.

Fig. 13.7: Example of adding an SNMP trap.

The main SNMP page will then be shown, now including the trap configuration details as shown in Fig. 13.8

To add a second entry again click the Add new trap destination button at the bottom of the SNMP Trap configuration table. An example of adding a second entry is shown in Fig. 13.9.

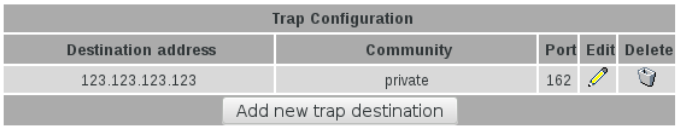


Fig. 13.8: The SNMP trap configuration details.

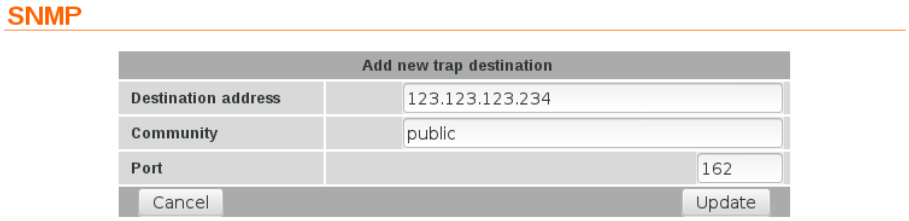


Fig. 13.9: Adding a second entry to the SNMP Trap list.

Click the Update button to add the entry to the table. The SNMP Trap configuration table will now include the new entry as shown in Fig. 13.10.

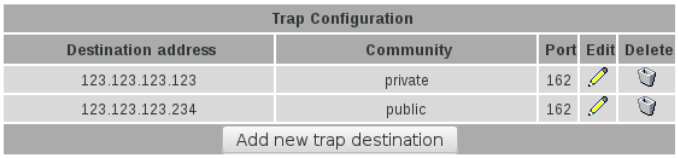


Fig. 13.10: SNMP Trap list showing two entries.

13.4.5 Editing an SNMP Trap Entry

The details for an SNMP Trap can be edited by clicking the icon in the **Edit** column, the details for the SNMP Trap will be shown as above in the Add new SNMP Trap example in Fig. 13.7. Changes can be made then click the Update button to save or click the Cancel button to exit and not save any changes.

As an example, to edit the second SNMP Trap entry in the table, click the icon in the second row of the table. To change the IP Address to 123.123.234.234, changes were made as shown in Fig. 13.11.

To save the changes click the Update button or to cancel any changes made click the Cancel button. The main page will again be displayed as shown in Fig. 13.12, with the changes for entry 2 added to the table.

13.4.6 Deleting an SNMP Trap entry

An SNMP Trap entry can be deleted by clicking the icon in the **Delete** column of the SNMP Trap table, a confirmation pop-up box will be displayed asking for confirmation of the delete. After deletion the SNMP Trap table on the main page will be updated.

For example, to delete SNMP Trap entry 2 from the table shown in Fig. 13.12, click the icon in row 2 of the table.

A warning box will then be displayed as shown in Fig. 13.13. Click the Ok button to confirm the deletion.

The main page will again be displayed as shown in Fig. 13.14, with entry 2 no longer included in the table.

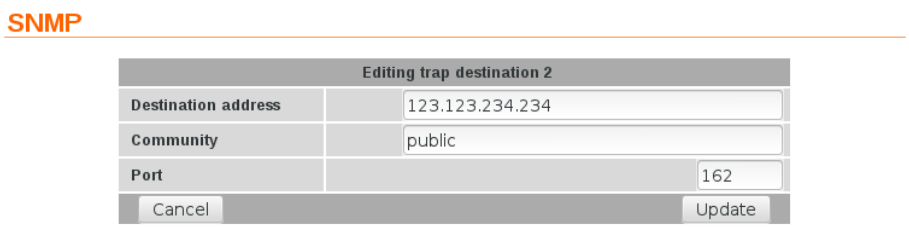


Fig. 13.11: Editing an SNMP Trap entry.

Fig. 13.12: List after editing SNMP Trap entry.

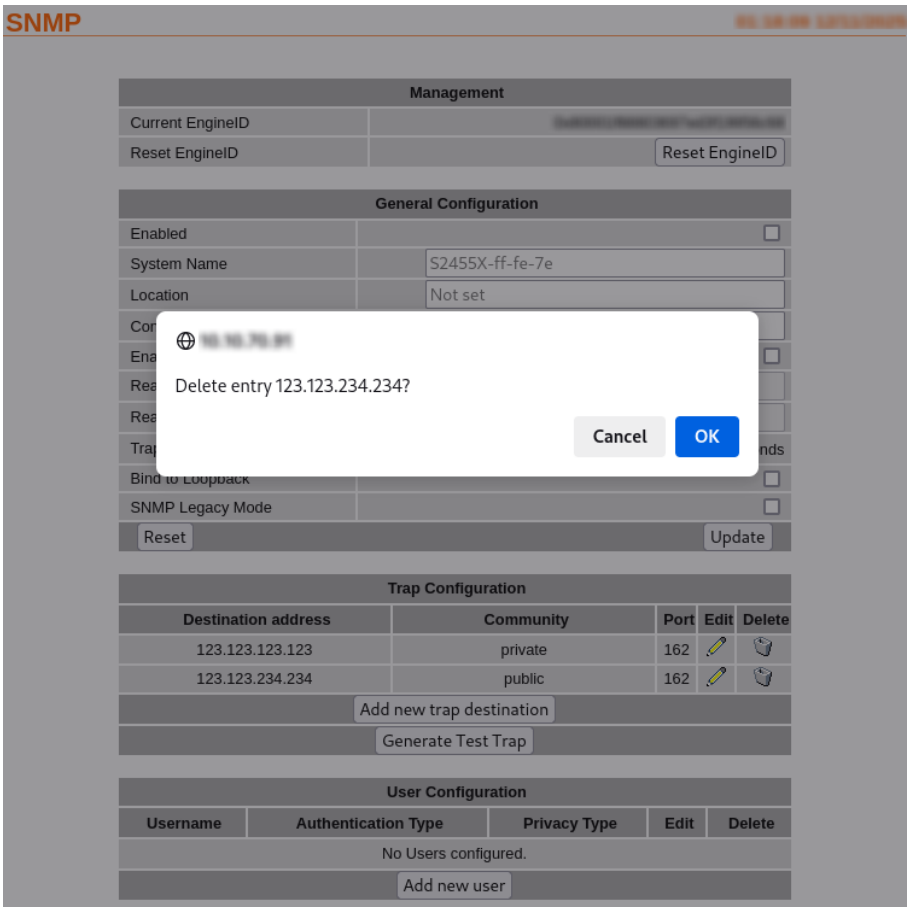


Fig. 13.13: Deleting an SNMP Trap entry.

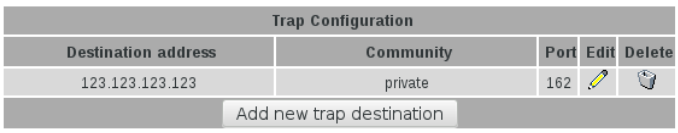


Fig. 13.14: The SNMP Trap table after deleting entry.

13.4.7 User Configuration

SNMPv3 provides a secure environment for the management of systems, this requires the identification of SNMP entities to facilitate communication only between known SNMP entities. Each SNMP entity has an identifier called the SNMP EngineID, and SNMP communication is possible only if an SNMP entity knows the identity of its peer. Users are defined for read and/or write access. This section describes the SNMP user configuration.

To add a new user click the Add new user button a page similar to that shown in Fig. 13.15 will appear.

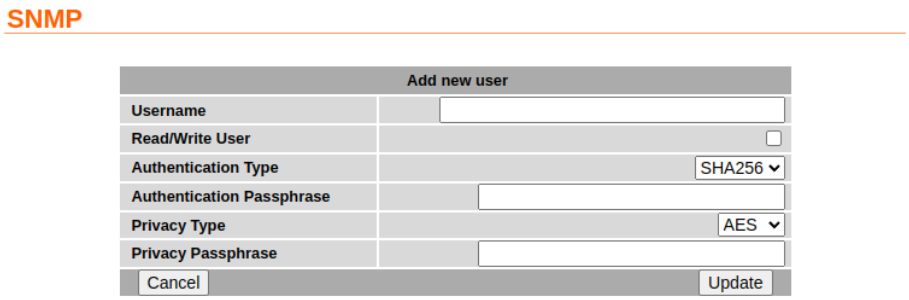


Fig. 13.15: The SNMP add user configuration page.

The following fields can be set:

Username
The user-name for the new user.

Read/Write User
Check to enable read / write access for the user. Leave un-checked for read only access.

Authentication Type
Choose the authentication type.

Options are:

None
No authentication type.

MD5
Message-Digest algorithm

SHA1
Secure Hash Algorithm 1

SHA-224
Secure Hash Algorithm 2 - 224 bit digest (hash value).

SHA-256
Secure Hash Algorithm 2 - 256 bit digest (hash value).

SHA-384
Secure Hash Algorithm 2 - 384 bit digest (hash value).

SHA-512
Secure Hash Algorithm 2 - 512 bit digest (hash value).

> **Note**
>
> For security it is recommended to use a SHA2 hash.

> **Warning**
>
> MD5 & SHA1 are not recommended as these hash algorithms are not considered secure.

Authentication Passphrase
Enter the authentication passphrase

Privacy Type
Choose the privacy type. Options:

None
No privacy type.

AES
Advanced Encryption Standard.

DES
Data Encryption Standard.

Privacy Passphrase
Enter a the privacy passphrase.

Click the Update button to save the new user configuration.

13.4.8 Example of Adding an SNMP User

To add a new entry click the Add new user button a page similar to that shown in Fig. 13.16 will appear. Add the details for the user as shown, then click Update to save the changes.

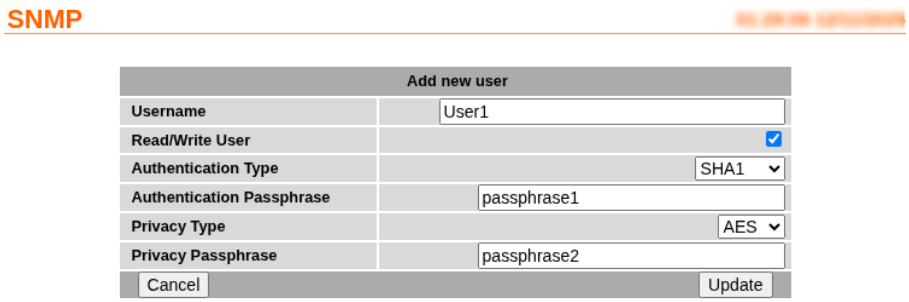


Fig. 13.16: Example of adding a new SNMP user.

The main SNMP page will then be shown, now including the user details as shown in Fig. 13.17.

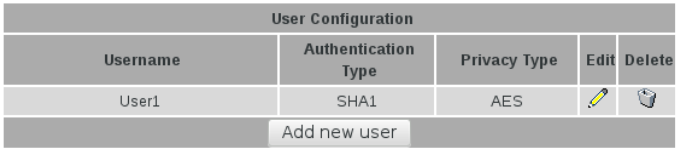


Fig. 13.17: The example SNMP user details on the main SNMP page.

To add a second entry again click the Add new user button at the bottom of the SNMP User configuration table. An example of adding a second entry is shown in Fig. 13.18.

Click the Update button to add the entry to the table.

The SNMP User configuration table will now include the new entry as shown in Fig. 13.19.

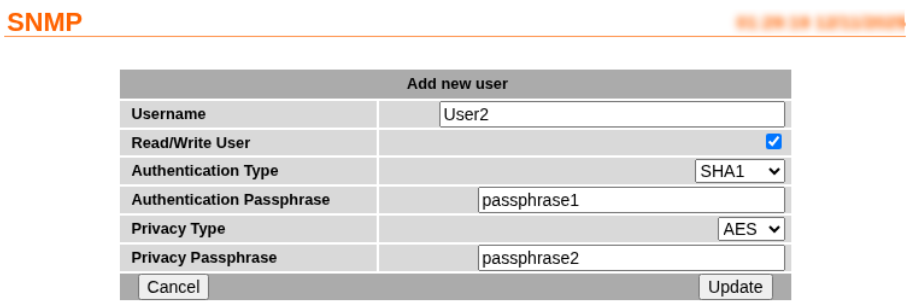


Fig. 13.18: Example of adding a second entry to the SNMP User list.

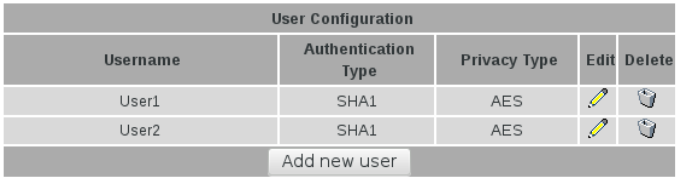


Fig. 13.19: SNMP user list showing two entries.

13.4.9 Editing an SNMP User Entry

The details for an SNMP User can be edited by clicking the icon in the **Edit** column, the details for the SNMP user will be shown as above in the Add new SNMP user example in Fig. 13.16. Changes can be made then click the Update button to save or click the Cancel button to exit and not save any changes. For security the pass-phrases are not displayed and cannot be edited. To change a passphrase the entire passphrase will need to re-entered.

As an example, to edit the second SNMP User entry in the table, click the icon in the second row of the table. The passphrases can now be changed. Changes were made as shown in Fig. 13.20.

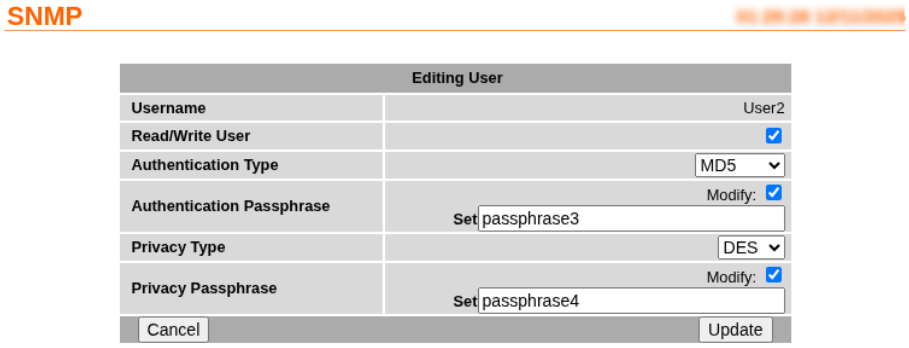


Fig. 13.20: Editing an SNMP User entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button.

The main page will again be displayed as shown in Fig. 13.21, with the changes for entry 2 added to the table.

13.4.10 Deleting an SNMP User entry

An SNMP User entry can be deleted by clicking the icon in the **Delete** column of the SNMP User table, corresponding to the User Entry to be deleted. A confirmation pop-up box will be displayed asking for confirmation of the delete. After deletion the SNMP User table on the main page will be updated.

For example, to delete SNMP User entry 2 from the table shown in Fig. 13.21, click the icon in row 2 of the

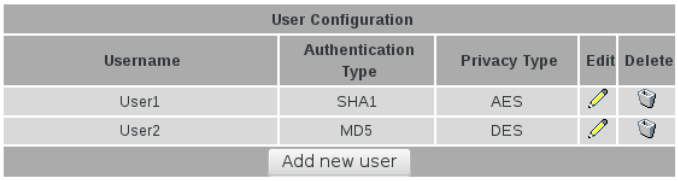


Fig. 13.21: List after editing SNMP User entry.

table. A warning box will now be displayed as shown in Fig. 13.22. Click the Ok button to confirm the deletion.

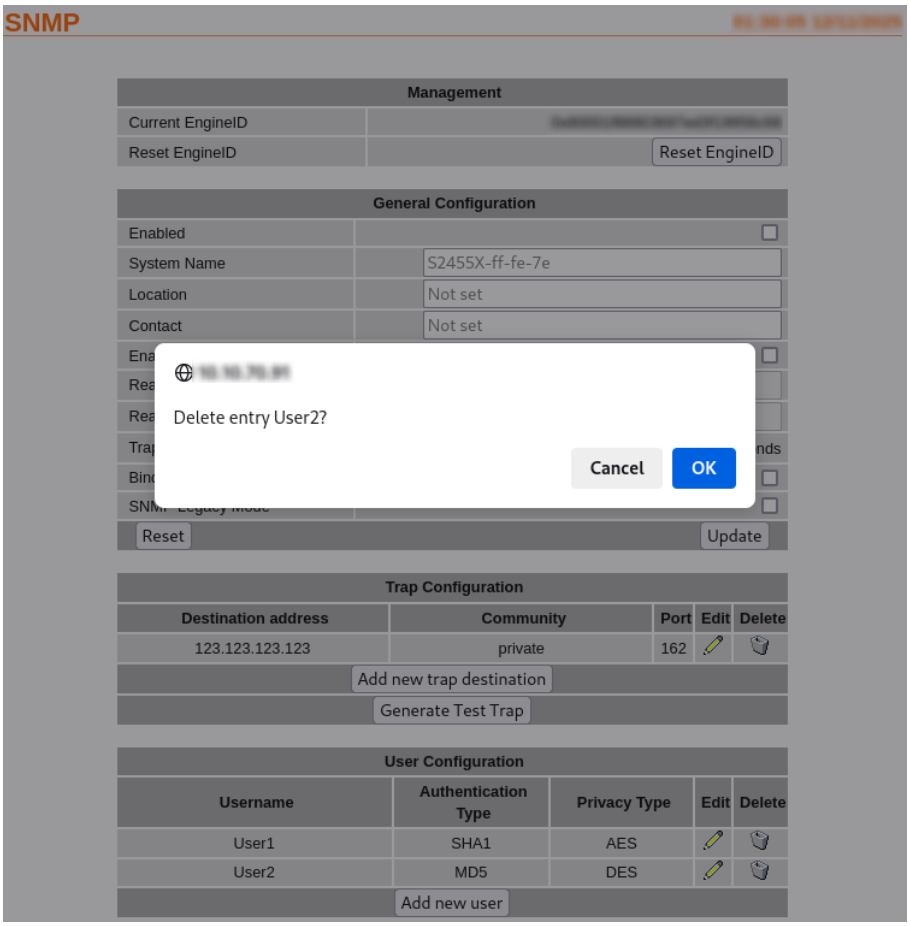


Fig. 13.22: Deleting an SNMP User entry.

The main page will again be displayed as shown in Fig. 13.23, with the entry 2 no longer included in the table.

13.5 DNP3

The modem can be configured to operate as a DNP3 outstation for reporting of the modem's state. Information such as the current connection status and RF level are available via DNP3 and, on models with GPIO, the GPIO can also be read and written. The options for these can be found by selecting *Management→DNP3*. The DNP3 page is shown in Fig. 13.24.

13.5.1 Configuring the outstation

The following can be set for the outstation:

Outstation mode

The outstation supports the following outstation modes:

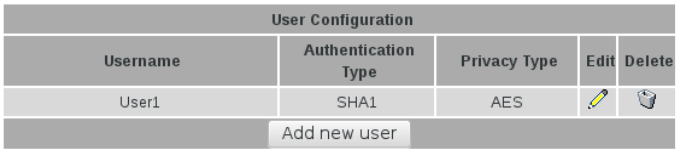


Fig. 13.23: The SNMP User table after deleting entry.

DNP3

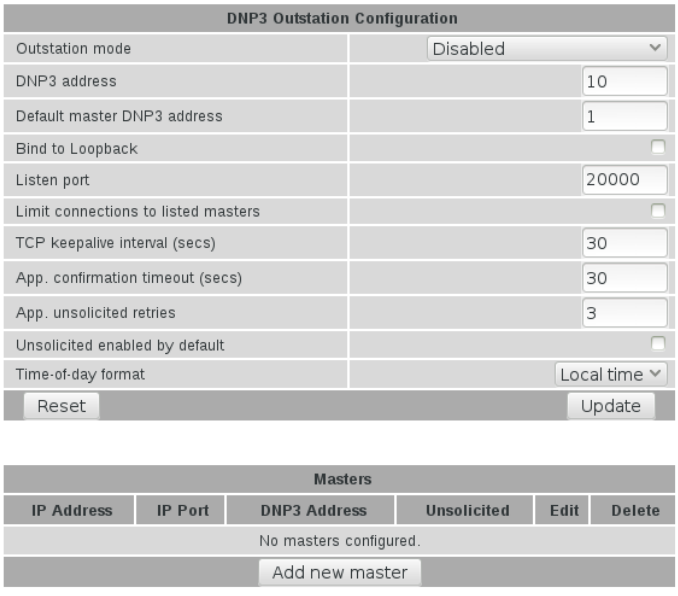


Fig. 13.24: The DNP3 outstation configuration page

Disabled
The outstation will not function.

TCP listen endpoint
The outstation will accept TCP connections from a DNP3 master.

TCP dual endpoint
The outstation will accept TCP connections from a DNP3 master. It will also establish a connection should an event occur while no master is connected.

UDP (datagram) endpoint
The outstation can be polled by a DNP3 master using UDP. Events will also be transmitted to the master via UDP.

DNP3 address
This is the DNP3 link-layer address for the outstation.

Default master DNP3 address
This is the address that will be used for TCP keep-alives if the DNP3 master address for a connection is currently unknown.

Listen port
This is the IP port number that the outstation will accept connections. The default DNP3 port number is 20000.

Limit connections to listed masters
When set, only masters whose IP addresses are listed in the masters table will be allowed to connect.

TCP keepalive interval (secs)
To detect dead TCP connections, the outstation will periodically send DNP3 polls to request the link status. If the master fails to respond, the connection will be closed. This field determines after what idle period (in seconds) that link status messages will be generated.

App. confirmation timeout (secs)
This is the time-out (in seconds) that will be used while waiting to receive an application level confirmation from a DNP3 master.

App. unsolicited retries
This is the number of times the outstation will retry sending unsolicited responses, should no confirmation be received from a master.

Unsolicited enabled by default
When this option is not set, the modem will not send any unsolicited responses until an ENABLE_UNSOLICITED (function code 20) message is received from a master. With this option set, the outstation will default to having unsolicited responses enabled.

Time-of-day format
This field determines the time format used in events. When set to UTC, the outstation will adjust all times by the system time zone setting (see section 5.2.4).

Click the Update button to save and commit the changes.

13.5.2 Adding a DNP3 master

Details of the DNP3 masters can be configured to allow limiting of connections or to enable unsolicited responses.

To configure the information about a new DNP3 master, click the Add new master button. A page similar to the shown in Fig. 13.25 will be presented.

The following fields can be set for each master:

Master IP address
The IP address of the DNP3 master.

Master IP port
The IP port number the master receives unsolicited responses on.

Fig. 13.25: The Add DNP3 master configuration page.

DNP3 address
The DNP3 link-layer address of the master.

Unsolicited receiver
When set, the master will receive unsolicited responses from the outstation.

Click the Update button to save the new master.

13.5.3 Example of Adding a DNP3 Master

To add a new entry click the Add new master button. A page similar to that shown in Fig. 13.26 will appear. Add the details for the DNP3 Master as shown, then click the Update button to save the changes.

Fig. 13.26: Example of adding a DNP3 Master.

The main DNP3 page will then be shown, now including the DNP3 Master details as shown in Fig. 13.27.

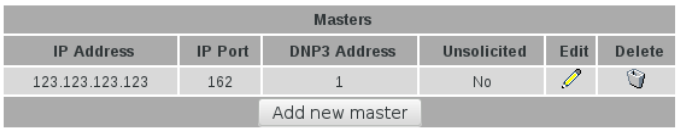


Fig. 13.27: The DNP3 Master list after adding new master.

To add a second entry again click the Add new master button at the bottom of the DNP3 Masters table. An example of adding a second entry is shown in Fig. 13.28.

Click the Update button to add the entry to the table. The DNP3 Master list will now include the new entry as shown in Fig. 13.29.

13.5.4 Editing a DNP3 Master Entry

The details for the DNP3 Master can be edited by clicking the  icon in the **Edit** column, the details for the DNP3 master will be shown as above in the Add new master example in Fig. 13.26.

Changes can be made, once complete, click the Update button to save or click the Cancel button to exit and not save any changes.

Fig. 13.28: Adding a second entry to the DNP3 master list.

Fig. 13.29: DNP3 Master list showing two entries.

As an example, to edit the second DNP3 Master entry in the table, click the  icon in the second row of the table. To change the DNP3 address to 2, changes were made as shown in Fig. 13.29.

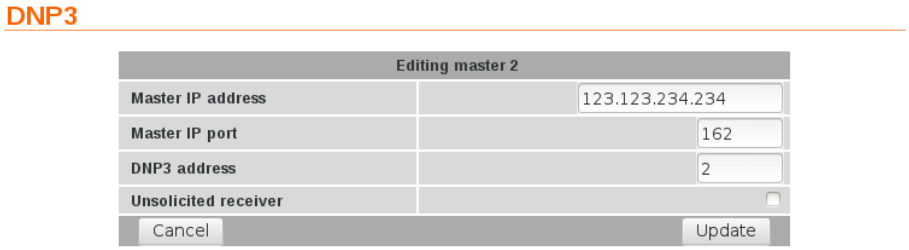


Fig. 13.30: Editing an DNP3 Master entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button . The main page will again be displayed as shown in Fig. 13.31, with the changes for entry 2 added to the table.

13.5.5 Deleting a DNP3 Master entry

A DNP3 Master entry can be deleted by clicking the  icon in the **Delete** column of the DNP3 Masters table. A confirmation pop-up box will be displayed asking for confirmation of the delete. After deletion the DNP3 table on the main page will be updated.

For example, to delete DNP3 Master entry 2 from the table shown in Fig. 13.31, click the  icon in the row for DNP Address 2. A warning box will now be displayed as shown if Fig. 13.32. Click the button icon in row 2 of the table.

The main page will again be displayed as shown in Fig. 13.33, with the entry 2 no longer included in the table.

13.6 SMS

The SMS page is used to configure the general SMS settings which include the SMS Distribution list and the SMS rate control. The page menu is accessed by selecting *Management→SMS*. The page is shown in Fig. 13.34.

Fig. 13.31: List after editing DNP3 Master entry.

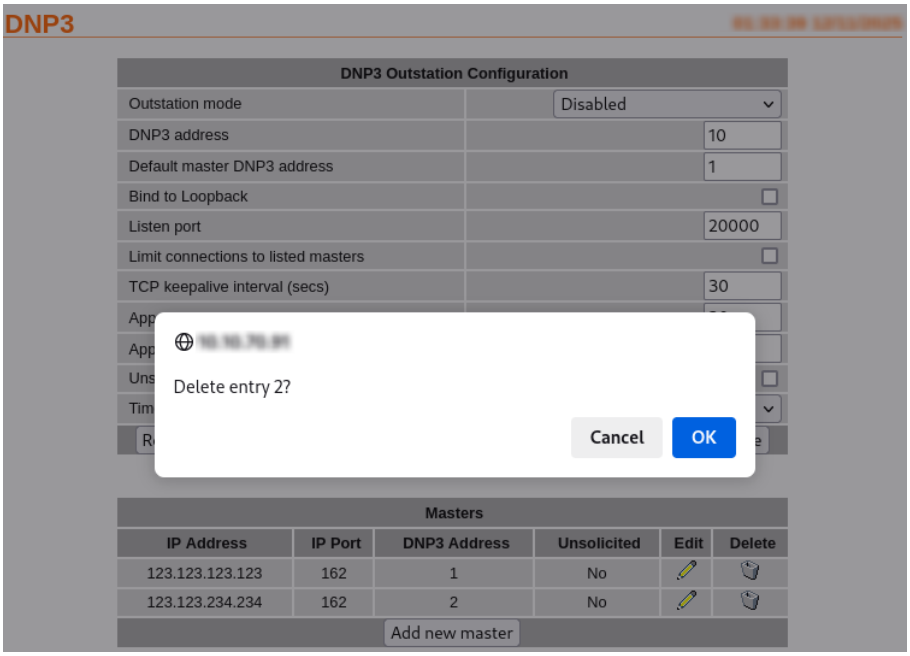


Fig. 13.32: Deleting an DNP3 Master entry.

Fig. 13.33: The DNP3 Master list after deleting entry.

13.6.1 SMS Control

The SMS Control section is used to configure global SMS settings including rate limiting of SMS and global sequence numbers.

The settings are:

Rate limit notifications
Used to set the maximum number of SMS which can be sent within a given time. This can be used to prevent an event trigger which changes more frequently than expected from generating a large number of messages. The timer starts at the time the first SMS is sent and resets once the number of seconds configured has elapsed.

The Format is:
Max. <number> SMS events per <time> seconds.

Where:
<Number> Is the maximum number of SMS events which can be sent for the time period; and

<time> Is the time period in seconds.

Add global sequence numbers
Check to enable the inclusion of a sequence number in each SMS.

> **Note**
>
> The global sequence number is set to 1 at boot time and increments by 1 for each message sent. If the unit is powered off or re-booted the global sequence number will be reset to 1.

Click Update button to save changes.

13.6.2 SMS Distribution List

The SMS distribution list section lists the current numbers to which SMSes will be sent and allows entries to be added, edited and deleted.

The fields of the table are:

Label
A text label for the entry.

Phone Number
The phone to which the SMS will be sent.

Enabled
Check to enable this entry.

Edit
Click the  icon to edit the entry.

Delete
Click the  icon to delete the entry.

13.6.3 SMS Entry Options

To access the SMS Entry Options click the button at the bottom of the SMS distribution list table. The following page will be displayed:

To create a new entry complete the fields which have the following meaning:

Label
A text label for the entry.

Fig. 13.34: The SMS configuration page.

Phone Number
The phone to which the SMS will be sent.

> **Note**
>
> The phone number must be in the form: +<country code><phone number>
>
> For example +61432123123
>
> If a number is entered with a 0 as the first digit +61 will automatically be added to the number and the 0 will be removed.

Enabled
Check to enable this entry.

When finished click the Update button to save the changes.

13.6.4 Adding a New SMS Entry

To add a new entry click the Add new destination button at the bottom of the SMS distribution list table. The Add new SMS destination page as shown in Fig. 13.34 will be displayed.

An example of an entry is shown in Fig. 13.35, in this case the entry will be labelled Test and the phone number is 0411123456.

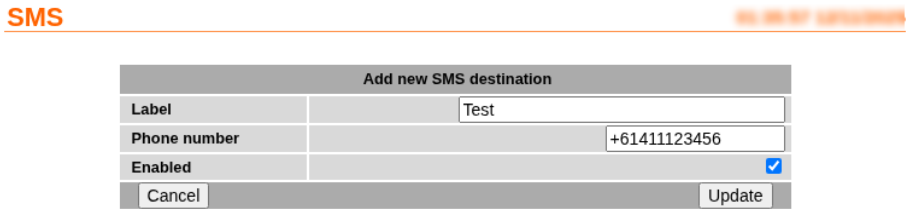


Fig. 13.35: An example of adding an SMS entry.

Once the changes have made click the Update button to save the entry. The SMS distribution list page will be displayed again now with the new entry as shown in Fig. 13.36.

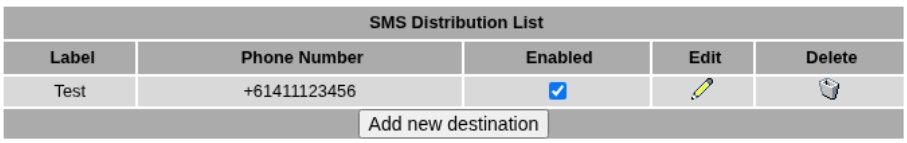


Fig. 13.36: The SMS entry has been added to the list.

To add a second entry again click the Add new destination button at the bottom of the SMS distribution list table.

An example of adding a second entry is shown in Fig. 13.37, in this case the label is called Test2 and the phone number is +61432123456.

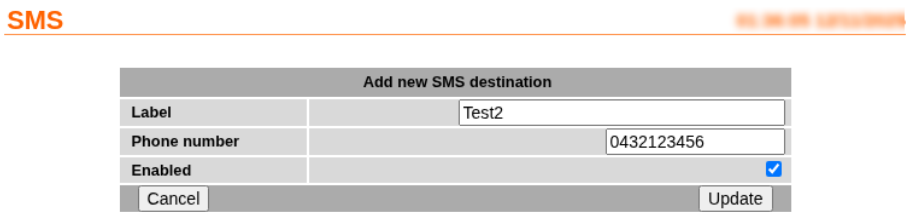


Fig. 13.37: Adding a second SMS entry to the distribution list.

Click the Update button to add the entry to the table.

The SMS distribution list will now include the new entry as shown in Fig. 13.38.

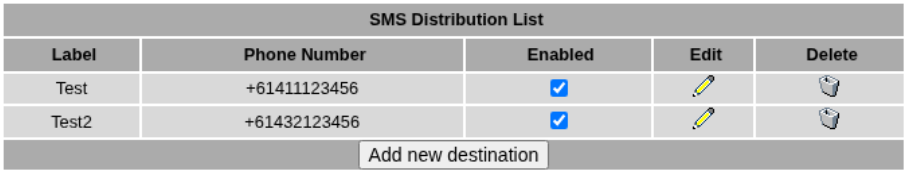


Fig. 13.38: SMS distribution list showing two entries.

13.6.5 Editing an SMS Entry

An SMS entry can be edited by clicking the icon in the **Edit** column of the entry to be changed. Once clicked, the details of the entry will be displayed in the same table as when creating a new SMS entry.

As an example, to edit the second SMS entry in the table, click the icon in the second row of the table. Change the phone number of the entry to +61432123456, as shown in Fig. 13.39.

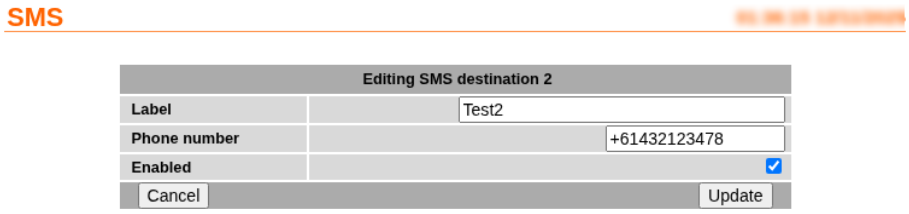


Fig. 13.39: An example of Editing SMS entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button.

The main page will again be displayed as shown in Fig. 13.40, with the changes for entry 2 added to the table.

13.6.6 Deleting an SMS entry

An SMS entry can be deleted by clicking the icon in the **Delete** column of the entry to be deleted. A warning box will be displayed. Click the OK to confirm the deletion.

For example, to delete SMS entry 2 from the table shown in Fig. 13.40, click the icon in row 2 of the table. A warning box will now be displayed as shown if Fig. 13.41. Click the OK button.

The main page will again be displayed as shown in Fig. 13.42, with the entry 2 no longer included in the table.

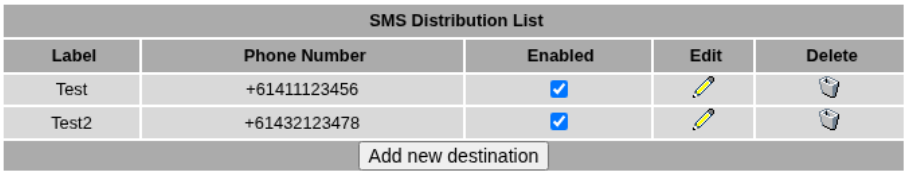


Fig. 13.40: SMS list after editing SMS entry.

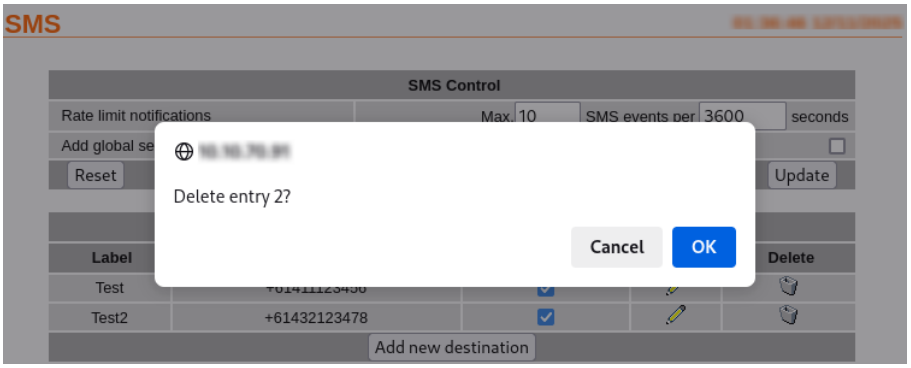


Fig. 13.41: Deleting an SMS entry.

13.7 Email

The Email page is used to configure the general Email settings which include the SMTP Server setting and the message rate control. The page menu is accessed by selecting *Management* → *Email* the page is shown in Fig. 13.43.

13.7.1 SMTP Server Configuration

The first section is used for the SMTP Server configuration.

This is the configuration for connecting to the server which will used for outgoing email:

SMTP server
: The fully qualified host-name or IP address of the server.

SMTP server port
: The server port number. (Default 25)

From address:
: The email address which will appear in the emails sent.

Enable TLS
: When enabled, the TLS will be used connect to the SMTP server.

Authenticate method
: Select the SMTP authentication method. Options are:

  None
  : no authentication.

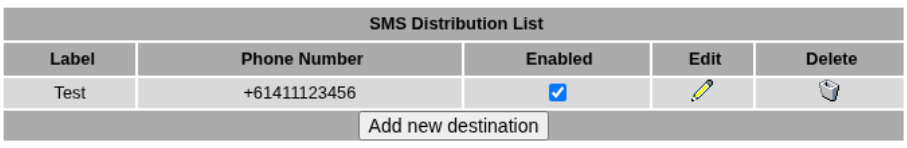


Fig. 13.42: SMS distribution list after deleting SMS entry.

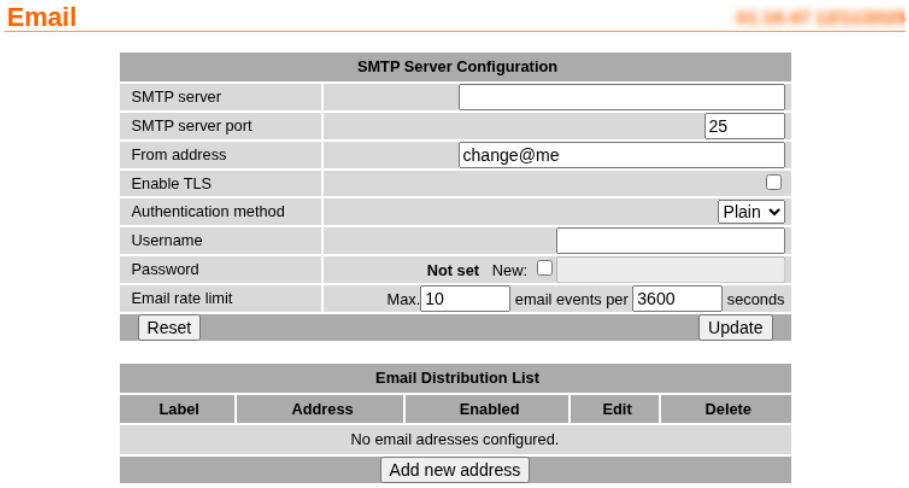


Fig. 13.43: The Email settings page.

Plain
Username and password authentication.

The Username and Password fields below are only active when the method is not None.

Username
The user-name used for authenticating with the server.

Password
The password used for authenticating with the server. To set the password first check the New check-box.

Email rate limit
Used to set the maximum number of email messages which can be sent within a given time. This can be used to prevent an event trigger which changes more frequently than expected from generating a large number of messages. The timer starts at the time the first email is sent and resets once the number of seconds configured has elapsed.

The Format is: Max. <number> email events per <time> seconds.

Where:

<Number>
Is the maximum number of email events which can be sent for the time period; and

<time>
Is the time period in seconds.

Click the Update button to save and commit changes.

13.7.2 Email Distribution List

The Email distribution list section lists the current numbers to which emails will be sent and allows entries to be added, edited and deleted.

The fields of the table are: Label A text label for the entry.

Address
The email address to which the emails will be sent.

Enabled
Check to enable this entry.

Edit Click the  icon to edit the entry. Delete Click the icon to delete the entry.

13.7.3 Email entry options

To access the Email Entry Options click the Add new address button at the bottom of the Email distribution list table. The page shown in Fig. 13.44 will be displayed:

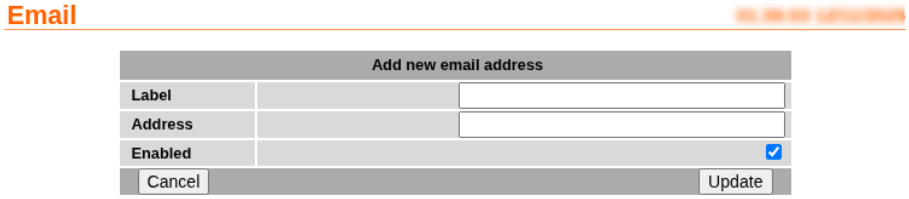


Fig. 13.44: Add new email address.

To create a new entry complete the fields which have the following meaning:

Label
A text label for the entry.

Address
The email address to which the emails will be sent.

Enabled
Check to enable this entry.

When finished click the Update button to save the changes.

13.7.4 Adding a New Email Entry

To add a new entry click the Add new address button at the bottom of the Email distribution list table. The Add new email address page as shown in Fig. 13.44 will be displayed.

An example of an entry is shown in Fig. 13.45, in this case the entry will be labelled Test and the address is test@example.com.

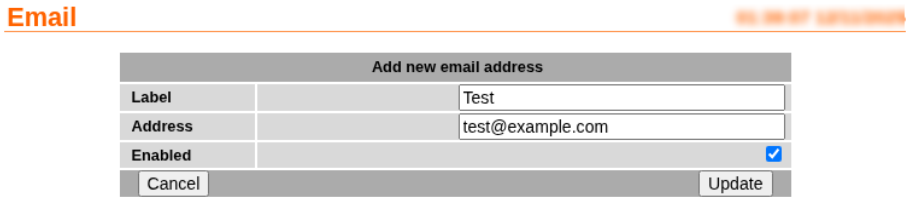


Fig. 13.45: An example of adding an email entry.

Once the changes have made click the Update button to save the entry.

The email distribution list page will be displayed again now with the new entry as shown in Fig. 13.46.

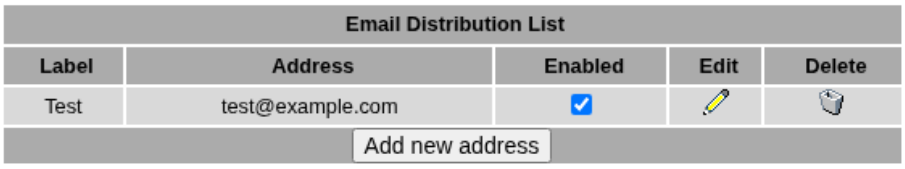


Fig. 13.46: The email entry has been added to the list.

To add a second entry again click the Add new address button at the bottom of the email distribution list table.

An example of adding a second entry is shown in Fig. 13.47, in this case the label is called Test2 and the address is test2@example.com.

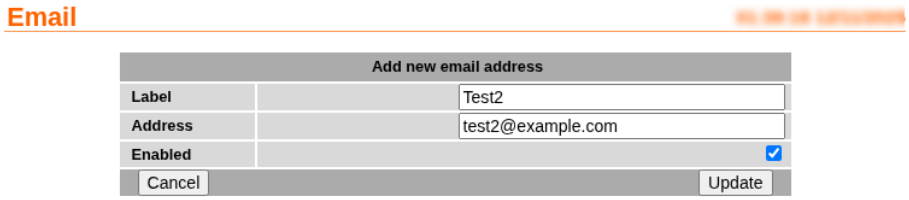


Fig. 13.47: Adding a second email entry to the distribution list.

Click the Update button to add the entry to the table.

The email distribution list will now include the new entry as shown in Fig. 13.48.

Fig. 13.48: The email distribution list showing two entries.

13.7.5 Editing an Email Entry

An entry can be edited by clicking the icon in the **Edit** column of the entry to be changed. Once clicked, the details of the entry will be displayed in the same table as when creating a new email address.

As an example, to edit the second email entry in the table, click the icon in the second row of the table. The address of the entry can now be changed to test2@email.com, as shown in Fig. 13.49.

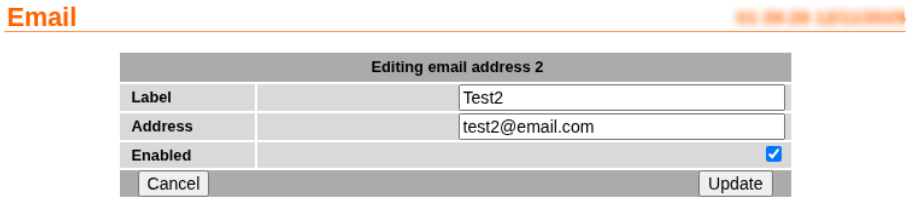


Fig. 13.49: Editing an email entry.

To save the changes click the Update button or to cancel any changes made click the Cancel button. The main page will again be displayed as shown in Fig. 13.50, with the changes for entry 2 included in the table.

13.7.6 Deleting an Email entry

An email entry can be deleted by clicking the icon in the Delete column of the entry to be deleted. A warning box will be displayed. Click the Ok button to confirm the deletion.

For example, to delete Email entry 2 from the table shown in Fig. 13.50, click the icon in row 2 of the table. A warning box will now be displayed as shown in Fig. 13.51. Click the Ok button to confirm the deletion.

The main page will again be displayed as shown in Fig. 13.52, with the entry 2 no longer included in the table.

Fig. 13.50: List after editing the email entry.

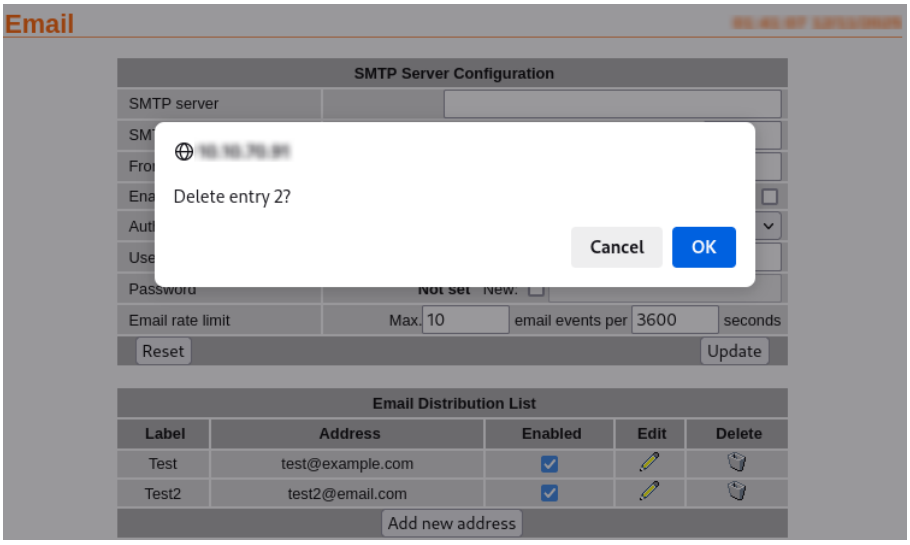


Fig. 13.51: Deleting an email entry.

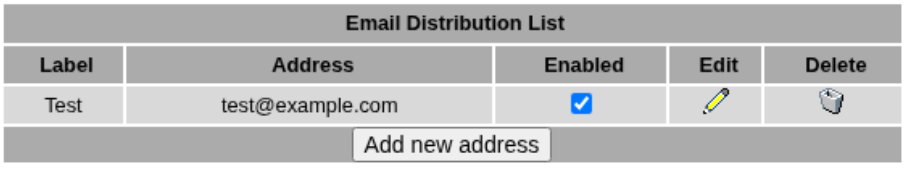


Fig. 13.52: The email distribution list after deleting email entry.

13.8 LLDP

The Link Layer Discovery Protocol (LLDP) page is enable LLDP on the modem.

The LLDP configuration page is accessed by selecting *Management→LLDP* from the main menu. A page similar to that shown in Fig. 13.53 will be displayed.

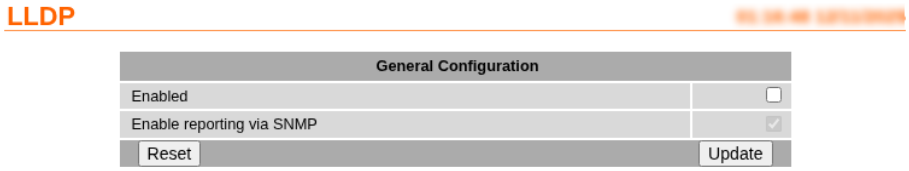


Fig. 13.53: The LLDP configuration page.

The LLDP page allows you to enable LLDP and reporting via SNMP.

13.9 CLI

The CLI page provides control of the Telnet and SSH services. The CLI page is accessed by selecting *Management→CLI* from the main menu. A page similar to that shown in Fig. 13.54 will be displayed.

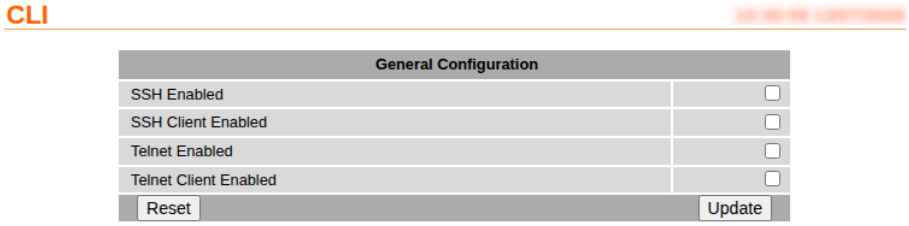


Fig. 13.54: The CLI configuration page.

The General Configuration options are:

SSH Enabled
Check to enabled the SSH server.

Enabling the SSH server will allow connections from a remote host to the unit using SSH.

SSH Client Enabled
Check to enable the SSH client.

Enabling the SSH client will allow connections from the unit to a remote device using SSH.

Telnet Enabled
Check to enabled the Telnet server.

Enabling the Telnet server will allow connections from a remote host to the unit using Telnet.

Telnet Client Enabled
Check to enable the Telnet client.

Enabling the Telnet client will allow connections from the unit to a remote device using Telnet.

APPENDIX

A.1 AT Commands

A.1.1 Introduction

This section presents the AT commands set supported by the modem emulator.

For details on configuring the modem emulator, refer to the *Modem Emulator* section of the *Serial Server* chapter.

Definitions

For the purposes of the present document, the following syntactical definitions apply:

<CR>
: Carriage return character, which value is specified with command S3.

<LF>
: Linefeed character, which value is specified with command S4.

<...>
: Name enclosed in angle brackets is a syntactical element. Brackets themselves do not appear in the command line.

[...]
: Optional subparameter of a command or an optional part of TA information response is enclosed in square brackets. Brackets themselves do not appear in the command line. When subparameter is not given in parameter type commands, new value equals to its previous value. In action type commands, action should be done on the basis of the recommended default setting of the subparameter.

Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP
: 3rd Generation Partnership Project

BCD
: Binary Coded Decimal

DCE
: Data Circuit-terminating Equipment

DCD
: Data Carrier Detect

DSR
: Data Set Ready

DTE
: Data Terminal Equipment

DTR
Data Terminal Ready

DTMF
Dual-Tone Multi-Frequency

ECNO
Received Energy per Chip divided by the power density in the band

EGPRS
Enhanced General Packet Radio Service

GPRS
General Packet Radio Service

GSM
Global System for Mobile Communications

HSDPA
High-Speed Downlink Packet Access

HSUPA
High-Speed Uplink Packet Access

IMEI
International Mobile Equipment Identity

IMEISV
International Mobile station Equipment Identity and Software Version number

IMSI
International Mobile Subscriber Identity

ITU
International Telecommunication Union

LTE
Long Term Evolution

ME
Mobile Equipment

MT
Mobile Terminal or Mobile Terminated

PDU
Protocol Data Unit

PIN
Personal Identification Number

PN
Pseudo-random Noise

PUK
PIN Unblocking Key

RSCP
Received Signal Code Power

RSRP
Reference Signal Received Power

RSRQ
Reference Signal Received Quality

RSSI
Received Signal Strength Indication

RXQUAL
Receive Quality

SIM
Subscriber Identity Module

SMS
Short Message Service

SMSC
Short Message Service Center

SVN
Software Version Number

TA
Terminal Adapter

TE
Terminal Equipment

UDI
Unrestricted Digital Information

UE
User Equipment

UICC
Universal Integrated Circuit Card

UMTS
Universal Mobile Telecommunications System

URC
Unsolicited Result Code

UTRAN
Universal Terrestrial Radio Access Network

AT Command Syntax

The "AT" or "at" prefix must be set at the beginning of each command line. To terminate a command line, enter <CR>. Commands are usually followed by a response that includes "<CR><LF><response><CR><LF>". Throughout this document, only the responses are presented, and "<CR><LF>" are omitted intentionally.

The AT Command Set implemented by the modem emulator is a combination of commands specified in the 3GPP TS 27.007, 3GPP TS 27.005 and ITU-T recommendation V.25ter specifications.

Command Line Format
A command line is made up of three elements:

- Prefix: the characters "AT" (or "at").
- Body: one or more individual commands. Space characters are ignored and may be used freely for formatting, unless embedded in numeric or string constants.
- Termination character: <CR> by default (configurable via S3).

Multiple commands may be concatenated in one command line. Basic syntax commands can follow one another without any separator. Extended syntax commands must be separated from a preceding extended command by a semicolon (";").

To repeat the previous command line, send "A/" (or "a/"). No termination character is needed in this case.

Command Types
There are two fundamental types of commands:

Action commands
Invoke a particular function. They may be executed or tested.

Parameter commands
Store a value or values for later use. They may be set, read, or tested.

Every extended command has a test command (trailing =?) to test the existence of the command and to give information about the type of its subparameters. Parameter type commands also have a read command (trailing ?) to check the current values of subparameters. Action type commands do not store the values of any of their possible subparameters, and therefore do not have a read command.

All these AT commands can be split into three categories syntactically: basic, S parameter, and extended. They are listed as follows:

- Basic Syntax

  These AT commands have the format of "AT<x><n>", or "AT&<x><n>", where "<x>" is the command, and "<n>" is/are the argument(s) for that command. An example of this is "ATE<n>", which tells the DCE whether received characters should be echoed back to the DTE according to the value of "<n>". "<n>" is optional and a default will be used if it is missing.

  <x> is a single alphabetic character (or "&" followed by a single alphabetic character). <n> is a decimal integer; if expected but missing, the value 0 is assumed. Leading zeros are ignored.

- S Parameter Syntax

  These AT commands have the format of "ATS<n>=<m>", where "<n>" is the index of the S register to set, and "<m>" is the value to assign to it.

  S-parameters also support reading:

```
ATS<n>?       Read current value (response: three-digit decimal)
ATS<n>=<m>    Set to new value
```

- Extended Syntax

  These commands can be operated in several modes:

  Test Command
  Used to query the supported parameter range or values of the command.

```
AT+<cmd>=?
```

  Read Command
  Used to query the current parameter settings of the command. Available only for parameter type commands. Action type commands do not store subparameter values and therefore do not have a read command.

```
AT+<cmd>?
```

  Write Command
  Used to set user-definable parameter values.

```
AT+<cmd>=<p1>[,<p2>,...,<pn>]
```

  Execution Command
  Used to execute the command with no parameters.

```
AT+<cmd>
```

  When multiple values (compound values) are used, they are separated by commas. If an intermediate value is omitted (default assumed), the comma separator must still be present; however, trailing commas may be omitted if all remaining values are also omitted.

Response Format
Responses consist of optional information text and final result codes.

There are two types of final result codes: regular and extended. Regular final result codes include “OK”, “ERROR” etc. Extended result codes include “+CME ERROR: <err>” and “+CMS ERROR: <err>” etc.

The format of information text and result codes depends on two settings: the V command (verbose vs. numeric format) and +CMEE (error reporting mode).

V command: verbose vs. numeric format

The V command controls the formatting of information text and regular result codes.

When V1 is active (default), both information text and result codes are framed with <CR><LF> before and after the text:

> Information response: <CR><LF><text><CR><LF> Result code: <CR><LF><verbose code><CR><LF>

When V0 is active, information text is followed by <CR><LF> only (no leading <CR><LF>), and result codes are sent as a numeric value followed by <CR> only (no <LF>):

> Information response: <text><CR><LF> Result code: <numeric code><CR>

+CMEE: error reporting mode

The +CMEE setting controls how errors are reported.

When +CMEE=0 (disabled, default), the regular result code “ERROR” is returned for all errors, including those related to invalid syntax, invalid parameters, and mobile equipment (ME) functionality.

When +CMEE=1 (enabled), extended result codes are used for errors related to ME functionality, while regular result codes are still used for other errors (e.g. syntax errors). The extended result code format is:

> <CR><LF>+<code>: <value><CR><LF>

where <code> is the error category (e.g. “CME ERROR”) and <value> is the numeric error code.

Combined formatting

The following summarises the response format under each combination of V and +CMEE settings.

Verbose mode (V1) with +CMEE=1:

> Information response: <CR><LF><text><CR><LF> Extended result code: <CR><LF>+<code>: <value><CR><LF>

Numeric mode (V0) with +CMEE=1:

> Information response: <text><CR><LF> Extended result code: <CR><LF>+<code>: <value><CR><LF>

A.1.2 General Commands

ATI Display Product Identification Information

ATI command delivers a product information text.

ATI
Display Product Identification Information

Execution Command

```
ATI
```

Response
TA issues product information text.

```
<product info>

OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<product info>
Product information text

Example

```
ATI
Serial Modem

OK
```

AT+GMI Request Manufacturer Identification

AT+GMI returns a manufacturer identification text. See also: AT+CGMI.

AT+GMI
Request Manufacturer Identification

Test Command

```
AT+GMI=?
```

Response

```
OK
```

Execution Command

```
AT+GMI
```

Response
TA reports one or more lines of information text which permit the user to identify the manufacturer.

```
<manufacturer>
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<manufacturer>
Manufacturer identification text

Example

```
AT+GMI
Cybertec
OK
```

AT+GMM Request TA Model Identification

AT+GMM returns a product model identification text. The command is identical with AT+CGMM.

AT+GMM
Request TA Model Identification

Test Command

```
AT+GMM=?
```

Response

```
OK
```

Execution Command

```
AT+GMM
```

Response
TA returns a product model identification text.

```
<model>
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<model>
Product model identification text

Example

```
AT+GMM
Cybertec Series 2455X
OK
```

AT+GMR Request TA Revision Identification of Software Release

AT+GMR delivers a product firmware version identification. The command is identical with AT+CGMR.

AT+GMR
Request TA Revision Identification of Software Release

Test Command

```
AT+GMR=?
```

Response

```
OK
```

Execution Command

```
AT+GMR
```

Response
TA reports one or more lines of information text which permit the user to identify the revision of software release.

```
<revision>
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<revision>
Revision of software release

Example

```
AT+GMR
1.9.10.0
OK
```

AT+CGMI Request Manufacturer Identification

AT+CGMI returns a manufacturer identification text. See also: AT+GMI.

AT+CGMI
Request Manufacturer Identification

Test Command

```
AT+CGMI=?
```

Response

```
OK
```

Execution Command

```
AT+CGMI
```

Response
TA returns manufacturer identification text.

```
<manufacturer>
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<manufacturer>
Manufacturer identification text

Example

```
AT+CGMI
Cybertec
OK
```

AT+CGMM Request Model Identification

AT+CGMM returns a product model identification text. The command is identical with AT+GMM.

AT+CGMM
Request Model Identification

Test Command

```
AT+CGMM=?
```

Response

```
OK
```

Execution Command

```
AT+CGMM
```

Response
TA returns product model identification text.

```
<model>
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<model>
Product model identification text

Example

```
AT+CGMM
Series 2455X
OK
```

AT+CGMR Request TA Revision Identification of Software Release

AT+CGMR delivers a product firmware version identification. The command is identical with AT+GMR.

AT+CGMR
Request TA Revision Identification of Software Release

Test Command

```
AT+CGMR=?
```

Response

```
OK
```

Execution Command

```
AT+CGMR
```

Response
TA returns identification text of product software version.

```
<revision>
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<revision>
Identification text of product software version

Example

```
AT+CGMR
1.8.7.1
OK
```

AT+GSN Request International Mobile Equipment Identity (IMEI)

AT+GSN returns the International Mobile Equipment Identity (IMEI). The command is identical with AT+CGSN.

AT+GSN
Request International Mobile Equipment Identity (IMEI)

Test Command

```
AT+GSN=?
```

Response

```
OK
```

Execution Command

```
AT+GSN
```

Response
TA reports the IMEI (International Mobile Equipment Identity) number in information text which permits the user to identify the individual ME device.

```
<IMEI>
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<IMEI>
IMEI of the telephone

Note

The serial number (IMEI) varies with the individual ME device.

AT+CGSN Request Product Serial Number Identification

AT+CGSN returns International Mobile Equipment Identity (IMEI).

AT+CGSN
Request Product Serial Number Identification

Test Command

```
AT+CGSN=?
```

Response

```
+CGSN: (0-3)

OK
```

Execution Command

```
AT+CGSN
```

Response
TA returns the product serial number, IMEI, IMEISV or SVN according to the <snt>.

When <snt>=0

```
<sn>
OK
```

When <snt>=1

```
+CGSN: "<imei>"
OK
```

When <snt>=2

```
+CGSN: "<imeisv>"
OK
```

When <snt>=3

```
+CGSN: "<svn>"
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<snt>
Serial number type (optional parameter)

0
Return product serial number (default if omitted)

1
Return IMEI (International Mobile station Equipment Identity)

2
Return IMEISV (International Mobile station Equipment Identity and Software Version number)

3
Return SVN (Software Version Number)

<sn>
Serial number string (format depends on <snt> value)

Example

```
AT+CGSN=0          //Request product serial number or IMEI
12345
OK
AT+CGSN=1          //Request IMEI
+CGSN: "866989053330061"
OK
AT+CGSN=2          //Request IMEISV
+CGSN: "8669890533300600"
OK
AT+CGSN=3          //Request SVN
+CGSN: "00"
OK
```

Note

When <snt> is 0 or omitted, the product serial number returned is

- IMEI for wireless units.
- Unit serial number for non-wireless units.

AT&F Set all Current Parameters to Manufacturer Defaults

AT&F resets AT command settings to their factory default values.

AT&F
Set all Current Parameters to Manufacturer Defaults

Execution Command

```
AT&F[<value>]
```

Response
TA sets all current parameters to the manufacturer defined profile. See Table 8: Factory Default Settings Restorable with AT&F.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<value>

0
Set all TA parameters to manufacturer defaults

AT&V Display Current Configuration

AT&V displays the current settings of several AT command parameters, including the single-letter AT command parameters which are not readable otherwise.

AT&V
Display Current Configuration

Execution Command

```
AT&V
```

Response
TA returns the current parameter setting

```
OK
```

Maximum Response Time
300ms

> **Note**
>
> This command is only implemented for compatibility.

AT&W Store Current Parameters to User Defined Profile

AT&W stores the current AT command settings to a user defined profile in non-volatile memory.

AT&W
Store Current Parameters to User Defined Profile

Execution Command

```
AT&W[<n>]
```

Response
TA stores the current parameter settings in the user defined profile.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0
Profile number to store current parameters

ATZ Set all Current Parameters to User Defined Profile

ATZ restores the current AT command settings to the user defined profile in non-volatile memory, if one was stored with AT&W before. Any additional AT command on the same command line may be ignored.

ATZ
Set all Current Parameters to User Defined Profile

Execution Command

```
ATZ[<value>]
```

Response

TA sets all current parameters to the user defined profile. See Table 10: AT Command Settings Storable with ATZ.

```
OK
```

Maximum Response Time

300ms

Reference

ITU-T Rec. V.250 (07/2003)

Parameter

<value>

0

Reset to profile number 0

ATQ Set Result Code Presentation Mode

ATQ controls whether the result code is transmitted to the TE. Other information text transmitted as response is not affected.

ATQ

Set Result Code Presentation Mode

Execution Command

```
ATQ<n>
```

Response

This parameter setting determines whether or not the TA transmits any result code to the TE. Information text transmitted in response is not affected by this setting.

If <n>=0:

```
OK
```

If <n>=1:

(none)

Maximum Response Time

300ms

Reference

ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0

TA transmits result code

1

Result codes are suppressed and not transmitted

ATV TA Response Format

This command determines the contents of header and trailer transmitted with AT command result codes and information responses.

The result codes, their numeric equivalents and brief descriptions of the use of each are listed in the following table.

ATV

TA Response Format

Execution Command

```
ATV<value>
```

Response

This parameter setting determines the contents of the header and trailer transmitted with result codes and information responses.

When <value>=0

```
0
```

When <value>=1

```
OK
```

Maximum Response Time

300ms

Reference

ITU-T Rec. V.250 (07/2003)

Parameter

<value>

0

Information response:
<text><CR><LF>

Short result code format:
<numeric code><CR>

1

Information response:
<CR><LF><text><CR><LF>

Long result code format:
<CR><LF><verbose code><CR><LF>

Example

```
ATV1        //Set <value>=1
OK
AT+CSQ
+CSQ: 30,99

OK          //When <value>=1 result code is OK
ATV0        //Set <value>=0
0
AT+CSQ
+CSQ: 30,99
0           //When <value>=0 result code is 0
```

ATE Set Command Echo Mode

ATE controls if the module echoes characters received from TE during AT command state.

ATE
Set Command Echo Mode

Execution Command

```
ATE<value>
```

Response
This setting determines whether or not the TA echoes characters received from TE during command state.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<value>

0
Echo mode OFF

1
Echo mode ON

A/ Repeat Previous Command Line

A/ repeats previous AT command line, and "/" acts as the line terminating character.

A/
Repeat Previous Command Line

Execution Command

```
A/
```

Response
Repeat the previous command

Reference
ITU-T Rec. V.250 (07/2003)

Example

```
ATI
Serial Modem

OK
A/
Serial Modem

OK
```

ATS3 Set Command Line Termination Character

ATS3 determines the character recognized by the module to terminate an incoming command line. It is also generated for result codes and information text, along with character value set via ATS4.

ATS3
Set Command Line Termination Character

Read Command

```
ATS3?
```

Response

```
<n>

OK
```

Write Command

```
ATS3=<n>
```

Response
This parameter setting determines the character recognized by TA to terminate an incoming command line. The TA also returns this character in output.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0-13-127
Command line termination character (Default 13=<CR>)

ATS4 Set Response Formatting Character

ATS4 determines the character generated by the module for result code and information text, along with the command line termination character set via ATS3.

ATS4
Set Response Formatting Character

Read Command

```
ATS4?
```

Response

```
<n>

OK
```

Write Command

```
ATS4=<n>
```

Response
This parameter setting determines the character generated by the TA for result code and information text.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0-10-127
Response formatting character (Default 10=<LF>)

ATS5 Set Command Line Editing Character

ATS5 determines the character value used by the module to delete the immediately preceding character from the AT command line (i.e. equates to backspace key).

ATS5
Set Command Line Editing Character

Read Command

```
ATS5?
```

Response

```
<n>

OK
```

Write Command

```
ATS5=<n>
```

Response
This parameter setting determines the character recognized by TA as a request to delete the immediately preceding character from the command line.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0-8-127
Response editing character (Default 8=<Backspace>)

ATX Set CONNECT Result Code Format and Monitor Call Progress

ATX determines whether or not the module transmits particular result codes to the TE. It also controls whether or not the module verifies the presence of a dial tone when it begins dialing, and whether or not engaged tone (busy signal) detection is enabled.

ATX
Set CONNECT Result Code Format and Monitor Call Progress

Execution Command

```
ATX<value>
```

Response
This parameter setting determines whether or not the TA detected the presence of dial tone and busy signal and whether or not TA transmits particular result codes.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<value>

0
CONNECT result code only returned, dial tone and busy detection are both disabled

1
CONNECT<text> result code only returned, dial tone and busy detection are both disabled

2
CONNECT<text> result code returned, dial tone detection is enabled, busy detection is disabled

3
CONNECT<text> result code returned, dial tone detection is disabled, busy detection is enabled

4
CONNECT<text> result code returned, dial tone and busy detection are both enabled

AT+CMEE Error Message Format

AT+CMEE controls the format of error result codes: "ERROR", error numbers or verbose messages as

"+CME ERROR: <err>" and "+CMS ERROR: <err>".

AT+CMEE
Error Message Format

Test Command

```
AT+CMEE=?
```

Response

```
+CMEE: (list of supported <n>s)

OK
```

Read Command

```
AT+CMEE?
```

Response

```
+CMEE: <n>

OK
```

Write Command

```
AT+CMEE=<n>
```

Response

TA disables or enables the use of result code +CME ERROR: <err> as an indication of an error related to the functionality of the ME.

```
OK
```

Maximum Response Time

300ms

Reference

3GPP TS 27.007

Parameter

<n>

0

Disable result code

1

Enable result code and use numeric values

Example

```
AT+CMEE=0       //Disable result code
OK
AT+CPIN?
ERROR           //Only "ERROR" will be displayed
AT+CMEE=1       //Enable error result code with numeric values
OK
AT+CPIN?
+CME ERROR: 10
```

AT+CSCS Select TE Character Set

AT+CSCS write command informs the module which character set is used by the TE. This enables the UE to convert character strings correctly between TE and UE character sets.

AT+CSCS

Select TE Character Set

Test Command

```
AT+CSCS=?
```

Response

```
+CSCS: (list of supported <chset>s)

OK
```

Read Command

```
AT+CSCS?
```

Response

```
+CSCS: <chset>

OK
```

Write Command

```
AT+CSCS=<chset>
```

Response

Set character set <chset> which is used by the TE. The TA can then convert character strings correctly between the TE and ME character sets.

```
OK
```

Maximum Response Time

300ms

Reference

3GPP TS 27.007

Parameter

<chset>

"IRA" International reference alphabet

"GSM"

GSM default alphabet

"HEX"

Hexdecimal representation of underlying data

"UTF-8"

UTF-8 alphabet

"PCCP437"

PC code page 437

"LATIN1"

ISO 8859-1 Latin Alphabet No. 1

Note

The value of character set is not persistent across module resets.

The default character set is UTF-8 .

Example

```
AT+CSCS=?
+CSCS: ("IRA","GSM","HEX","UTF-8","PCCP437","LATIN1")

OK
AT+CSCS?
+CSCS: "UTF-8"

OK
```

AT+GCAP Capabilities List

AT+GCAP returns the capabilities of the module.

AT+GCAP
Capabilities List

Test Command

```
AT+GCAP=?
```

Response

```
OK
```

Execution Command

```
AT+GCAP
```

Response
TA returns a list of supported capabilities.

```
+GCAP: <capability1>,<capability2>,...

OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

AT+FCLASS Select Active Service Class

AT+FCLASS selects the active service class of the module.

AT+FCLASS
Select Active Service Class

Test Command

```
AT+FCLASS=?
```

Response

```
+FCLASS: (list of supported <n>s)

OK
```

Read Command

```
AT+FCLASS?
```

Response

```
+FCLASS: <n>

OK
```

Write Command

```
AT+FCLASS=<n>
```

Response

```
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<n>

0
data

AT+GCI Country of installation

AT+GCI sets or queries the country code of the module's installation location.

AT+GCI
Country of installation

Test Command

```
AT+GCI=?
```

Response

```
+GCI: (list of supported <cc>s)

OK
```

Read Command

```
AT+GCI?
```

Response

```
+GCI: <cc>

OK
```

Write Command

```
AT+GCI=<cc>
```

Response
This parameter setting determines the country code of the module's installation location.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

A.1.3 Serial Interface Control Commands

AT&C Set DCD Function Mode

AT&C controls the behavior of the UE's DCD line.

AT&C
Set DCD Function Mode

Execution Command

```
AT&C[<value>]
```

Response
This parameter determines how the state of circuit 109(DCD) relates to the detection of received line signal from the distant end.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<value>

0
DCD line is always ON

1
DCD line is ON only in the presence of data carrier

AT&D Set DTR Function Mode

AT&D determines how the UE responds if DTR line is changed from ON to OFF condition during online data mode.

AT&D
Set DTR Function Mode

Execution Command

```
AT&D[<value>]
```

Response
This parameter determines how the TA responds when circuit 108/2 (DTR) is changed from ON to OFF condition during Maximum Response Time data mode.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<value>

0
TA ignores status on DTR

1
ON->OFF on DTR: Change to command mode while remaining the connected call

2
ON->OFF on DTR: Disconnect data call, and change to command mode. During state DTR = OFF, auto-answer function is disabled

AT&S Data Set Ready (DSR) Control

AT&S controls the behavior of the UE's DSR line.

AT&S
Data Set Ready (DSR) Control

Execution Command

```
AT&S[<value>]
```

Response
This parameter determines how the state of circuit 104(DSR) relates to the detection of received line signal from the distant end.

```
OK
```

Maximum Response Time
300ms

AT+IPR Set TE-TA Fixed Local Rate

AT+IPR is used to query and set the baud rate of the UART. The default baud rate value (<rate>) is 115200bps. <rate> setting will not be restored with AT&F.

AT+IPR
Set TE-TA Fixed Local Rate

Test Command

```
AT+IPR=?
```

Response

```
+IPR: (list of supported auto detectable <rate>s),(list of
supported fixed-only <rate>s)

OK
```

Read Command

```
AT+IPR?
```

Response

```
+IPR: <rate>

OK
```

Write Command

```
AT+IPR=<rate>
```

Response
This parameter setting determines the data rate of the TA on the serial interface. After the delivery of any result code associated with the current command line, the rate of command takes effect.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<rate>
Baud rate per second

- 300
- 600
- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- 115200
- 230400

Note

1. If a fixed baud rate is set, make sure that both TE (DTE, usually external processor) and TA (DCE, wireless module) are configured to the same rate.
2. The value of AT+IPR cannot be restored with AT&F and ATZ; but it is still storable with AT&W.
3. In multiplex mode, the baud rate cannot be changed by the write command AT+IPR=<rate>; and the setting is invalid and cannot be stored even if AT&W is executed after the write command.
4. A selected baud rate takes effect after the write commands are executed and acknowledged by "OK".

Example

```
AT+IPR=115200       //Set fixed baud rate to 115200bps
OK
AT&W                //Store current setting, that is, the serial communication
                    //speed is 115200bps after restarting module

OK
AT+IPR?
+IPR: 115200

OK
AT+IPR=115200;&W    //Set fixed baud rate to 115200bps and store current
                    //setting

OK
```

A.1.4 SIM Related Commands

AT+CIMI Request International Mobile Subscriber Identity (IMSI)

AT+CIMI requests the International Mobile Subscriber Identity (IMSI) which is intended to permit the TE to identify the individual SIM card or active application in the UICC (GSM or USIM) that is attached to MT.

AT+CIMI
Request International Mobile Subscriber Identity (IMSI)

Test Command

```
AT+CIMI=?
```

Response

```
OK
```

Execution Command

```
AT+CIMI
```

Response
TA returns <IMSI> for identifying the individual SIM which is attached to ME.

```
<IMSI>

OK
```

If error is related to ME functionality:

```
+CME ERROR: <err>
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<IMSI>
International Mobile Subscriber Identity (string without double quotes)

Example

```
AT+CIMI
460023210226023     //Query IMSI number of SIM which is attached to ME

OK
```

AT+CPIN Enter PIN

AT+CPIN is used to enter a password or query whether or not the module requires a password which is necessary before it can be operated (SIM PIN, SIM PUK, PH-SIM PIN, etc.).

AT+CPIN
Enter PIN

Test Command

```
AT+CPIN=?
```

Response

```
OK
```

Read Command

```
AT+CPIN?
```

Response

TA returns an alphanumeric string indicating whether or not some password is required.

```
+CPIN: <code>

OK
```

Write Command

```
AT+CPIN=<pin>[,<new pin>]
```

Response

TA stores a password which is necessary before it can be operated (SIM PIN, SIM PUK, etc.). If the PIN is to be entered twice, the TA shall automatically repeat the PIN. If no PIN request is pending, no action is taken and an error message,

```
+CME ERROR, is returned to TE.
```

If the PIN required is SIM PUK or SIM PUK2, the second pin is required. This second pin, <new pin>, is used to replace the old pin in the SIM.

```
OK
```

Maximum Response Time

5s

Reference

3GPP TS 27.007

Parameter

<code>

READY
MT is not pending for any password

SIM PIN
MT is waiting for SIM PIN to be given

SIM PUK
MT is waiting for SIM PUK to be given

SIM PIN2
MT is waiting for SIM PIN2 to be given

SIM PUK2
MT is waiting for SIM PUK2 to be given

PH-NET PIN
MT is waiting for network personalization password to be given

PH-NET PUK
MT is waiting for network personalization unblocking password to be given

PH-NETSUB PIN
MT is waiting for network subset personalization password to be given

PH-NETSUB PUK
MT is waiting for network subset personalization unblocking password to be given

PH-SP PIN
MT is waiting for service provider personalization password to be given

PH-SP PUK
MT is waiting for service provider personalization unblocking password to be given

PH-CORP PIN
MT is waiting for corporate personalization password to be given

PH-CORP PUK
MT is waiting for corporate personalization unblocking password to be given

<pin>
Password (string type). If the requested password was a PUK, such as SIM PUK1, PH-FSIM PUK or another password, then <pin> must be followed by <new pin>.

<new pin>
New password (string type) if the requested code was a PUK.

Example

```
//Enter PIN

AT+CPIN?
+CPIN: SIM PIN          //Query PIN code is locked

OK
AT+CPIN=1234            //Enter PIN
OK

+CPIN: READY
AT+CPIN?                //PIN has already been entered
+CPIN: READY

OK

//Enter PUK and PIN

AT+CPIN?

+CPIN: SIM PUK          //Query PUK code is locked

OK
AT+CPIN="26601934","1234"   //Enter PUK and new PIN password
OK

+CPIN: READY
AT+CPIN?
+CPIN: READY            //PUK has already been entered

OK
```

A.1.5 Network Service Commands

AT+CREG Network Registration

AT+CREG returns the network registration status. The write command sets whether or not to present URC.

AT+CREG
Network Registration

Test Command

```
AT+CREG=?
```

Response

```
+CREG: (list of supported <n>s)

OK
```

Read Command

```
AT+CREG?
```

Response

In Non-CDMA mode:

TA returns the status of result code presentation and an integer <stat> which shows whether the network has currently indicated the registration of the ME. Location information elements <lac> and <ci> are returned only when <n>=2 and ME is registered in the network.

```
+CREG: <n>,<stat>[,<lac>,<ci>[,<Act>]]

OK
```

If error is related to ME functionality:

```
+CME ERROR: <err>
```

Write Command

```
AT+CREG[=<n>]
```

Response

TA controls the presentation of an unsolicited result code

```
+CREG: <stat> when <n>=1 and there is a change in the ME
network registration status.

OK
```

Maximum Response Time

300ms

Reference

3GPP TS 27.007

Parameter

<n>

0

Disable network registration unsolicited result code

1

Enable network registration unsolicited result code +CREG: <stat>

2

Enable network registration unsolicited result code with location information +CREG: <stat>[,<lac>,<ci>[,<Act>]]

<stat>

0

Not registered, ME is not currently searching a new operator to register to

1
Registered, home network

2
Not registered, but ME is currently searching a new operator to register to

3
Registration denied

4
Unknown

5
Registered, roaming

<lac>
String type, two bytes location area code in hexadecimal format

<ci>
String type, two bytes cell ID in hexadecimal format

<Act>
Access technology selected

0
GSM

2
UTRAN

3
GSM W/EGPRS

4
UTRAN W/HSDPA

5
UTRAN W/HSUPA

6
UTRAN W/HSDPA and HSUPA

7
E-UTRAN

Example

```
AT+CREG=1
OK

+CREG: 1            //URC reports that ME has registered
AT+CREG=2           //Activates extended URC mode
OK

+CREG:  1,“D509”,”80D413D”,2                    //URC  reports  that  operator ␣
↪has  found  location  area  code
                                                //and cell ID
AT+CREG=1
OK

+CREG: 1                    //URC reports that ME has registered
AT+CREG=2                   //Activates extended URC mode
OK

AT+CREG?
```

(continues on next page)

(continued from previous page)

```
+CREG:  2,1,“3747”,”A23C2”,100                    //Query  the  system  ID, ␣
↪network  ID  and  BTS  ID  of  CDMA
                                                  //network
OK
```

AT+CSQ Signal Quality Report

AT+CSQ indicates the received signal strength <rssi> and the channel bit error rate <ber>.

AT+CSQ
Signal Quality Report

Test Command

```
AT+CSQ=?
```

Response

```
+CSQ: (list of supported <rssi>s),(list of supported <ber>s)

OK
```

Execution Command

```
AT+CSQ
```

Response

```
+CSQ: <rssi>,<ber>

OK
+CME ERROR: <err>
```

Execution Command returns received signal strength indication <rssi> and channel bit error rate <ber> from the ME. Test Command returns values supported by the TA.

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<rssi>

0
-113dBm or less

1
-111dBm

2...30
-109... -53dBm

31
-51dBm or greater

99
Not known or not detectable

100
-116dBm or less

101
-115dBm

102...190
-114...-26dBm

191
-25dBm or greater

199
Not known or not detectable

100~199
Extended to be used in TDSCDMA indicating received signal code power (RSCP)

<ber>
Channel bit error rate (in percent)

0...7
As RXQUAL values in the table in 3GPP TS 45.008 subclause 8.2.4

99
Not known or not detectable

Example

```
AT+CSQ=?
+CSQ: (0-31,99),(0-7,99)

OK
AT+CSQ
+CSQ: 28,99         //Returns that the current signal strength indication is 28␣
↪and
                    channel bit error rate is 99

OK
```

AT+CESQ Extended Signal Quality Report

AT+CESQ indicates the extended signal quality parameters.

AT+CESQ
Execution Command returns extended signal quality parameters from the ME. Test Command returns values supported by the TA.

Test Command

```
AT+CESQ=?
```

Response

```
+CESQ: (list of supported <rxlev>s),(list of supported <ber>s),
(list of supported <rscp>s),(list of supported <ecno>s),
(list of supported <rsrq>s),(list of supported <rsrp>s)

OK
```

Execution Command

```
AT+CESQ
```

Response

```
+CESQ: <rxlev>,<ber>,<rscp>,<ecno>,<rsrq>,<rsrp>

OK
+CME ERROR: <err>
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<rxlev>
Received signal level

0
-110dBm or less

1…63
-109… -48dBm

255
Not known or not detectable

<ber>
Channel bit error rate (in percent)

0…7
As RXQUAL values in the table in 3GPP TS 45.008 subclause 8.2.4

99
Not known or not detectable

<rscp>
Received signal code power

0
-120dBm or less

1…96
-119… -25dBm

255
Not known or not detectable

<ecno>
Ratio of the received energy per PN chip to the total received power spectral density (see 3GPP TS 25.133 sublause).

0
-24dB or less

1…49
-23…0dB

255
Not known or not detectable

<rsrq>
Reference signal received quality.

0
-20dB or less

1…34
-19.5… -3dB

255
Not known or not detectable

<rsrp>
Reference signal received power.

0
-140dBm or less

1...97
-139... -44dBm

255
Not known or not detectable

Example

```
AT+CESQ
+CESQ: 99,99,255,255,16,37

OK
```

A.1.6 Call Related Commands

ATA Answer an Incoming Call

ATA connects the module to an incoming voice or data call indicated by a "RING" URC.

ATA Answer an Incoming Call

Execution Command

```
ATA
```

Response
TA sends off-hook to the remote station. Response in case of data call, if successfully connected

```
CONNECT<text>
```

TA switches to data mode. Note: <text> outputs only when <value> >0 in ATX <value> parameter setting.

When TA returns to command mode after call release:

```
OK
```

Response in case of voice call, if successfully connected:

```
OK
```

Response if no connection:

```
NO CARRIER
```

Maximum Response Time
90s, determined by network.

Reference
ITU-T Rec. V.250 (07/2003)

Note

1. Any additional commands on the same command line are ignored.

2. This command may be aborted generally by receiving a character during execution. The aborting is not possible during some states of connection establishment such as handshaking.
3. See also ATX.

Example

```
RING            //A voice call is ringing
AT+CLCC
+CLCC: 1,0,0,1,0,“”,128                         //PS call in LTE mode
+CLCC: 2,1,4,0,0,“02154450290”,129              //Incoming call

OK
ATA             //Accept the voice call with ATA
OK
```

ATD Mobile Originated Call to Dial a Number

ATD can be used to set up outgoing voice and data calls. Supplementary Services can also be controlled with ATD.

ATD Mobile Originated Call to Dial a Number

Execution Command

```
ATD<n>[<mgsm>][;]
```

Response

This command can be used to set up outgoing voice, data or FAX calls. It also serves to control supplementary services.

If no dial tone and (parameter setting ATX2 or ATX4):

```
NO DIALTONE
```

If busy and (parameter setting ATX3 or ATX4):

```
BUSY
```

If a connection cannot be established:

```
NO CARRIER
```

If connection is successful and non-voice call.

```
CONNECT<text>
```

TA switches to data mode. <text> outputs only when <value> >0 in ATX<value> parameter setting.

When TA returns to command mode after call release:

```
OK
```

If connection is successful and voice call:

```
OK
```

Maximum Response Time

5s, determined by network (AT+COLP=0).

Reference

ITU-T Rec. V.250 (07/2003)

Parameter

<n>

This field determines how the emulator will handle dial requests from the serial port (ATDxxxx commands). The dial address may be set to:

Fixed destination

Regardless of the value entered after the ATD command, the emulator will always connect to the host specified in the **Fixed destination address** and **Fixed destination port** fields.

From dial string

The emulator will parse the ATD command to extract the destination address and port number. The examples below show the two different formats that can be used to create a connection to the address 10.10.10.10 and port number 6001.

Dotted

Dial string is ATD 10.10.10.10:6001

Padded

Dial string is ATD 01001001001006001

From phone book

When a dial command is entered, the emulator will look up the modem's phone book and attempt to translate the number to an address and port number.

For more details on the phone book refer to *Phone Book*

Example

```
ATD10086;       //Dialing out the party's number

OK
```

ATH Disconnect Existing Connection

ATH disconnects circuit switched data calls or voice calls. AT+CHUP is also used to disconnect the voice call.

ATH Disconnect Existing Connection

Execution Command

```
ATH[n]
```

Response

Disconnect existing call by local TE from command line and terminate the call.

```
OK
```

Maximum Response Time

90s, determined by network.

Reference

ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0 Disconnect from line and terminate call

+++ Switch from Data Mode to Command Mode

The +++ character sequence causes the module to switch from data mode to AT command mode. It allows inputting AT commands while maintaining the data connection with the remote device.

+++

Switch from Data Mode to Command Mode

Execution Command

```
+++
```

Response

This command is only available when TA is in data mode. The“+++” character sequence causes the TA to cancel the data flow over the AT interface and switch to command mode. This allows you to enter AT command while maintaining the data connection with the remote server or, accordingly, the GPRS connection.

```
OK
```

Maximum Response Time

300ms

Reference

ITU-T Rec. V.250 (07/2003)

Note

1. To prevent the“+++” escape sequence from being misinterpreted as data, it should comply to following sequence: - Do not input any character within T1 time (1000ms) before inputting “+++”. - Input “+++” within 1000ms, and no other characters can be inputted during the time. - Do not input any character within T1 time (1000ms) after “+++” has been inputted. - Switch to command mode; otherwise return to step 1.
2. To return from command mode back to data mode: Enter ATO - Another way to change to command mode is through DTR, refer to AT&D command for details.

ATO Switch from Command Mode to Data Mode

ATO resumes the connection and switches back from command mode to data mode.

ATO

Switch from Command Mode to Data Mode

Execution Command

```
ATO[n]
```

Response

TA resumes the connection and switches back from command mode to data mode.

If connection is not successfully resumed:

```
NO CARRIER
```

Else

TA returns to data mode from command mode CONNECT

```
<text>
```

Maximum Response Time

300ms

Reference

ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0

Switch from command mode to data mode

Note

TA returns to data mode from command mode CONNECT <text>; <text> outputs only when <value> >0 in ATX<value> parameter setting.

ATS0 Set Number of Rings before Automatically Answering Call

ATS0 controls automatic answering mode for the incoming calls.

ATS0
Set Number of Rings before Automatically Answering Call

Read Command

```
ATS0?
```

Response

```
<n>

OK
```

Write Command

```
ATS0=<n>
```

Response
This parameter setting determines the number of rings before auto-answer.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0
Automatic answering is disabled

1-255
Enable automatic answering on the ring number specified

Note

If <n> is set too high, the calling party may hang up before the call is answered automatically.

Example

```
ATS0=3      //Set three rings before automatically answering a call
OK

RING        //Call coming

RING

RING        //Automatically answering the call after three rings
```

ATS7 Set Number of Seconds to Wait for Connection Completion

ATS7 specifies the amount of time to wait for the connection completion in case of answering or originating a call. If no connection is established during the time, the module disconnects from the line.

ATS7
Set Number of Seconds to Wait for Connection Completion

Read Command

```
ATS7?
```

Response

```
<n>

OK
```

Write Command

```
ATS7=<n>
```

Response
This parameter setting determines the amount of time to wait for the connection completion in case of answering or originating a call.

```
OK
```

Maximum Response Time
300ms

Reference
ITU-T Rec. V.250 (07/2003)

Parameter

<n>

0
Disabled

1-255
Number of seconds to wait for connection completion

ATS12 Escape Prompt Delay

ATS12 specifies the delay time for the escape sequence"+++" to be recognized when TA is in data mode.

ATS12
Escape Prompt Delay

Read Command

```
ATS12?
```

Response

```
<n>

OK
```

Write Command

```
ATS12=<n>
```

Response

This parameter setting determines the delay time for the escape sequence "+++" to be recognized when TA is in data mode.

```
OK
```

Maximum Response Time

300ms

Reference

ITU-T Rec. V.250 (07/2003)

Parameter

<n>

1-255

Delay time in fiftieth of a second.

AT+CBST Select Bearer Service Type

AT+CBST write command selects the bearer service <name>, the data rate <speed> and the connection element <ce> to be used when data calls are originated.

AT+CBST

Select Bearer Service Type

Test Command

```
AT+CBST=?
```

Response

```
+CBST: (list of supported <speed>s),(list of supported
<name>s),(list of supported <ce>s)

OK
```

Read Command

```
AT+CBST?
```

Response

```
+CBST: <speed>,<name>,<ce>

OK
```

Write Command

```
AT+CBST=[<speed>[,<name>[,<ce>]]]
```

Response

TA selects the bearer service <name> with data rate <speed>, and the connection element <ce> to be used when data calls are originated.

```
OK
```

Maximum Response Time

300ms

Reference

3GPP TS 27.007

Parameter

<speed>

0
Automatic speed selection

7
9600 bps (V.32)

12
9600 bps (V.34)

14
14400 bps (V.34)

16
28800 bps (V.34)

17
32000 bps (V.34)

39
9600 bps (V.120)

43
14400 bps (V.120)

48
28800 bps (V.120)

51
56000 bps (V.120)

71
9600 bps (V.110)

75
14400 bps (V.110)

80
28800 bps (V.110 or X.31 flag stuffing)

81
38400 bps (V.110 or X.31 flag stuffing)

83
56000 bps (V.110 or X.31 flag stuffing; this setting can be used in conjunction with asynchronous non-transparent UDI or RDI service in order to get FTM84 64000 bps (X.31 flag stuffing; this setting can be used in conjunction with asyn-chronous non-transparent UDI service in order to get FTM)

84
64000 bps (X.31 flag stuffing; this setting can be used in conjunction with asynchronous non-transparent UDI service in order to get FTM)

116
64000 bps (bit transparent)

134
64000 bps (multimedia)

<name>

0
Asynchronous Modem

1
Synchronous Modem

4
Asynchronous Modem (RDI)

<ce>

0
Transparent

1
Non-transparent

> **Note**
>
> 3GPP TS 22.002 lists the allowed combinations of the sub-parameters.

AT+CR Service Reporting Control

AT+CR controls the module whether or not to transmit an intermediate result code +CR: <serv> to the TE when a call is being set up.

If it is enabled, an intermediate result code is transmitted at the point during connect negotiation at which the TA has determined which speed and quality of service will be used, before any error control or data compression reports are transmitted, and before any final result code (e.g. CONNECT) is transmitted.

AT+CR
Service Reporting Control

Test Command

```
AT+CR=?
```

Response

```
+CR: (list of supported <mode>s)

OK
```

Read Command

```
AT+CR?
```

Response

```
+CR: <mode>

OK
```

Write Command

```
AT+CR=[<mode>]
```

Response
TA controls whether or not intermediate result code +CR: <serv> is returned from the TA to the TE when a call set up.

```
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<mode>

0
Disable

1
Enable

<serv>

ASYNC
Asynchronous transparent

SYNC
Synchronous transparent

REL ASYNC
Asynchronous non-transparent

REL SYNC
Synchronous non-transparent

GPRS
GPRS

A.1.7 Short Message Service Commands

AT+CSMS Select Message Service

AT+CSMS selects messaging service <service> and returns the types of messages supported by the ME.

AT+CSMS
Select Message Service

Test Command

```
AT+CSMS=?
```

Response

```
+CSMS: (list of supported <service>s)

OK
```

Read Command

```
AT+CSMS?
```

Response

```
+CSMS: <service>,<mt>,<mo>,<bm>

OK
```

Write Command

```
AT+CSMS=<service>
```

Response

```
+CSMS: <mt>,<mo>,<bm>

OK
```

If error is related to ME functionality:

```
+CMS ERROR: <err>
```

Maximum Response Time
300ms

Reference
3GPP TS 27.005

Parameter

<service>
Type of message service

0
3GPP TS 23.040 and 3GPP TS 23.041 (the syntax of SMS AT commands is compatible with 3GPP TS 27.005 Phase 2 version 4.7.0; Phase 2+ features which do not require new command syntax may be supported, e.g. correct routing of messages with new Phase 2+ data coding schemes).

1
3GPP TS 23.040 and 3GPP TS 23.041 (the syntax of SMS AT commands is compatible with 3GPP TS 27.005 Phase 2+ version; the requirement of <service> setting 1 is mentioned under corresponding command descriptions).

<mt>
Mobile terminated messages

0
Type not supported

1
Type supported

<mo>
Mobile originated messages

0
Type not supported

1
Type supported

<bm>
Broadcast type messages

0
Type not supported

1
Type supported

Example

```
AT+CSMS=?        //Test command
+CSMS: (0,1)

OK
AT+CSMS=1        //Set type of message service as 1
+CSMS: 1,1,1

OK
AT+CSMS?         //Read command
+CSMS: 1,1,1,1

OK
```

AT+CMGF Message Format

AT+CMGF specifies the input and output format of the short messages. <mode> indicates the format of messages used with send, list, read and write commands and unsolicited result codes resulting from received messages.

Mode can be either PDU mode (entire TP data units used) or text mode (headers and body of the messages given as separate parameters). Text mode uses the value of parameter <chset> specified by command AT+CSCS to inform the character set to be used in the message body in the TA-TE interface.

AT+CMGF
Message Format

Test Command

```
AT+CMGF=?
```

Response

```
+CMGF: (list of supported <mode>s)

OK
```

Read Command

```
AT+CMGF?
```

Response

```
+CMGF: <mode>

OK
```

Write Command

```
AT+CMGF[=<mode>]
```

Response
TA sets parameter to denote which kind of I/O format of messages is used.

```
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.005

Parameter

<mode>

0
PDU mode

1
Text mode

AT+CSCA Service Center Address

AT+CSCA write command updates the SMSC address when mobile originated SMS are transmitted. In text mode, the setting is used by write commands. In PDU mode, setting is used by the same commands, but only when the length of the SMSC address is coded into the <pdu> parameter which equals to zero.

AT+CSCA
Service Center Address

Test Command

```
AT+CSCA=?
```

Response

```
OK
```

Read Command

```
AT+CSCA?
```

Response

```
+CSCA: <sca>,<tosca>

OK
```

Write Command

```
AT+CSCA=<sca>[,<tosca>]
```

Response

```
OK
```

If error is related to ME functionality:

```
+CME ERROR: <err>
```

Maximum Response Time
300ms

Reference
3GPP TS 27.005

Parameter

<sca>
Service center address. 3GPP TS 24.011 RP SC address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in 3GPP TS 27.007); type of address is given by <tosca>.

<tosca>
Type of service center address. 3GPP TS 24.011 RP SC address Type-of-Address octet in integer format (default refer to <toda>).

Example

```
AT+CSCA="+8613800210500",145        //Set SMS service center address
OK
AT+CSCA?                            //Query SMS service center address
+CSCA: "+8613800210500",145

OK
```

AT+CSAS Save Settings

AT+CSAS saves settings which have been made by the +CSCA +CSMP and +CSCB commands in local non volatile memory.

AT+CSAS
Save Settings

Test Command

```
AT+CSAS=?
```

Response

```
OK
```

Write Command

```
AT+CSAS[=<profile>]
```

Parameter:

<profile>

0
it saves the settings to NVM (factory default).

1..n
SIM profile number; the value of n depends on the SIM and its max is 3.

Response

```
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.005

AT+CPMS Preferred Message Storage

AT+CPMS selects memory storages <mem1>,<mem2>and <mem3> to be used for reading, writing, etc.

AT+CPMS
Preferred Message Storage

Test Command

```
AT+CPMS=?
```

Response

```
+CPMS: (list of supported <mem1>s),(list of supported
<mem2>s),(list of supported <mem3>s)

OK
```

Read Command

```
AT+CPMS?
```

Response

```
+CPMS:
<mem1>,<used1>,<total1>,<mem2>,<used2>,<total2>,<m
em3>,<used3>,<total3>
OK
```

Write Command

```
AT+CPMS=<mem1>[,<mem2>[,<mem3>]]
```

Response

TA selects memory storages <mem1>, <mem2> and <mem3> to be used for reading, writing, etc.

```
+CPMS:
<used1>,<total1>,<used2>,<total2>,<used3>,<total3>

OK
```

If error is related to ME functionality:

```
+CMS ERROR: <err>
```

Maximum Response Time

300ms

Reference

3GPP TS 27.005

Parameter

<mem1>

Messages to be read and deleted from this memory storage

"SM"

SIM message storage

"ME"

Mobile equipment message storage

"MT"

Same as "ME" storage

<mem2>

Messages will be written and sent to this memory storage

"SM"

SIM message storage

"ME"

Mobile equipment message storage

"MT"

Same as "ME" storage

<mem3>

Received messages will be placed in this memory storage if routing to PC is not set (AT+CNMI)

"SM"

SIM message storage

"ME"

Mobile equipment message storage

"MT"

Same as "ME" storage

<usedx>

Integer type, number of current messages in <memx>

<totalx>

Integer type, total number of messages which can be stored in <memx>

Example

```
AT+CPMS?                    //Query the current SMS message storage
+CPMS: “ME”,0,255,“ME”,0,255,“ME”,0,255

OK
AT+CPMS=“SM”,“SM”,“SM”      //Set SMS message storage as “SM”
+CPMS: 0,50,0,50,0,50

OK
AT+CPMS?                    //Query the current SMS message storage
+CPMS: “SM”,0,50,“SM”,0,50,“SM”,0,50

OK
```

AT+CMGD Delete Message

AT+CMGD deletes a short message from the preferred message storage <mem1> location <index>. If <delflag> is presented and not set to 0, then the ME shall ignore <index> and follow the rules of <delflag> shown as below.

AT+CMGD
Delete Message

Test Command

```
AT+CMGD=?
```

Response

```
+CMGD: (list of supported <index>s),(list of supported
<delflag>s)

OK
```

Write Command

```
AT+CMGD=<index>[,<delflag>]
```

Response
TA deletes message from preferred message storage <mem1> location <index>.

```
OK
```

If error is related to ME functionality:

```
+CMS ERROR:<err>
```

Maximum Response Time
300ms.

Note: Operation of <delflag> depends on the storage of deleted messages.

Reference
3GPP TS 27.005

Parameter

<index>
Integer type, in the range of location numbers supported by the associated memory

<delflag>

0
Delete the message specified in <index>

1
Delete all read messages from <mem1> storage

2
Delete all read messages from <mem1> storage and sent mobile originated messages

3
Delete all read messages from <mem1> storage, sent and unsent mobile originated messages

4
Delete all messages from <mem1> storage

Example

```
AT+CMGD=1       //Delete the message specified in <index>=1
OK
AT+CMGD=1,4     //Delete all messages from <mem1> storage
OK
```

AT+CMGL List Messages

AT+CMGL read command returns messages with status value <stat> from preferred message storage <mem1> to the TE. If the status of the message is "REC UNREAD", the status in the storage changes to "REC READ". When executing command AT+CMGL without status value <stat>, it will report the list of SMS with "REC UNREAD" status.

AT+CMGL
List Messages

Test Command

```
AT+CMGL=?
```

Response

```
+CMGL: (list of supported <stat>s)

OK
```

Write Command

```
AT+CMGL[=<stat>]
```

Response
If text mode (+CMGF=1) and command successful: For SMS-SUBMITs and/or SMS-DELIVERs:

```
+CMGL:
<index>,<stat>,<oa/da>,[<alpha>],[<scts>][,<tooa/toda>,<length>]<CR><LF><data>[
↪<CR><LF>

+CMGL:
<index>,<stat>,<da/oa>,[<alpha>],[<scts>][,<tooa/toda>,<length>]<CR><LF><data>[..
↪.]]
```

For SMS-STATUS-REPORTs:

```
+CMGL:
<index>,<stat>,<fo>,<mr>,[<ra>],[<tora>],<scts>,<dt>,<st>[<CR><LF>
+CMGL:
<index>,<stat>,<fo>,<mr>,[<ra>],[<tora>],<scts>,<dt>,<st>[...]]
```

For SMS-COMMANDs:

```
+CMGL: <index>,<stat>,<fo>,<ct>[<CR><LF>
+CMGL: <index>,<stat>,<fo>,<ct>[...]]
```

For CBM storage:

```
+CMGL:<index>,<stat>,<sn>,<mid>,<page>,<pages><CR><LF><data>[<CR><LF>
+CMGL:
<index>,<stat>,<sn>,<mid>,<page>,<pages><CR><LF><data>[...]]

OK
```

Else if PDU mode (+CMGF=0) and command successful:

```
+CMGL:<index>,<stat>,[<alpha>],<length><CR><LF><pdu><CR><LF>
+CMGL:
<index>,<stat>,[alpha],<length><CR><LF><pdu>[...]]

OK
```

Execution Command

```
AT+CMGL
```

Response

List all messages with "REC UNREAD" status from message storage <mem1>; then status in the storage changes to "REC READ".

Maximum Response Time

300ms

Note: Operation of <stat> depends on the storage of listed messages.

Reference

3GPP TS 27.005

Parameter

<stat>

In text mode:

"REC UNREAD"
Received unread messages

"REC READ"
Received read messages

"STO UNSENT"
Stored unsent messages

"STO SENT"
Stored sent messages

"ALL"
All messages

In PDU mode:

0
Received unread messages

1
Received read messages

2
Stored unsent messages

3
Stored sent messages

4
All messages

<index>
Integer type, in the range of location numbers supported by the associated memory

<da>
Destination Address. 3GPP TS 23.040 TP-Destination-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in 3GPP TS 27.007); type of address is given by <toda>.

<oa>
Originating address. 3GPP TS 23.040 TP-Originating-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in TS 27.007); type of address is given by <tooa>.

<alpha>
String type alphanumeric representation of <da> or <oa> corresponding to the entry found in MT phonebook; implementation of this feature is manufacturer specified; the used character set should be the one selected with command Select TE Character Set AT+CSCS (see definition of this command in 3GPP TS 27.007).

<scts>
Service center time stamp. 3GPP TS 23.040 TP-Service-Centre-Time-Stamp in time-string format (refer to <dt>).

<toda>
Type of recipient address. 3GPP TS 24.011 TP-Recipient-Address Type-of-Address octet in integer format.

<tooa>
Type of originating address. 3GPP TS 24.011 TP-Originating-Address Type-of-Address octet in integer format (default refer to <toda>).

<length>
Message length, integer type, indicating in the text mode (AT+CMGF=1) the length of the message body <data> (or <cdata>) in characters; or in PDU mode (AT+CMGF=0) the length of the actual TP data unit in octets (i.e. the RP layer SMSC address octets are not counted in the length).

<data>
In the case of SMS: 3GPP TS 23.040 TP-User-Data in text mode responses; format:

- If <dcs>, indicates that 3GPP TS 23.038 GSM 7 bit default alphabet is used and <fo> indicates that 3GPP TS 23.040 TP-User-Data-Header-Indication is not set.
- If TE character set other than "HEX" (refer to command Select TE Character Set +CSCS in 3GPP TS 27.007): ME/TA converts GSM alphabet into current TE character set according to rules of Annex A.
- If TE character set is "HEX": ME/TA converts each 7-bit character of GSM 7 bit default alphabet into two IRA character long hexadecimal number (e.g. character (U+F050) (GSM 7 bit default alphabet 23) is presented as 17 (IRA 49 and 55)).
- If <dcs>, indicates that 8-bit or UCS2 data coding scheme is used, or <fo> indicates that 3GPP TS 23.040 TP-User-Data-Header-Indication is set: ME/TA converts each 8-bit octet into two IRA character long hexadecimal number (e.g. octet with integer value 42 is presented to TE as two characters 2A (IRA 50 and 65)).

In the case of CBS: 3GPP TS 23.041 CBM Content of Message in text mode responses; format:

- If <dcs>, indicates that 3GPP TS 23.038 GSM 7 bit default alphabet is used:

- If TE character set other than “HEX” (refer to command AT+CSCS in 3GPP TS27.007): ME/TA converts GSM alphabet into current TE character set according to rules of Annex A.
- If TE character set is “HEX”: ME/TA converts each 7-bit character of the GSM 7 bit default alphabet into two IRA character long hexadecimal number.
- If <dcs>, indicates that 8-bit or UCS2 data coding scheme is used: ME/TA converts each 8-bit octet into two IRA character long hexadecimal number.

<pdu>
In the case of SMS: 3GPP TS 24.011 SC address followed by 3GPP TS 23.040 TPDU in hexadecimal format: ME/TA converts each octet of TP data unit into two IRA character long hexadecimal number (e.g. octet with integer value 42 is presented to TE as two characters 2A (IRA 50 and 65)) 3GPP TS 27.007.

Note

The command in CDMA network now only supports Text mode.

Example

```
AT+CMGF=1                          //Set SMS message format as text mode
OK
AT+CMGL=“ALL”                      //List all messages from message storage
+CMGL: 1,“STO UNSENT”,“”,,

<This is a test>

+CMGL: 2,“STO UNSENT”,“”,,

<This is a test>

OK
```

AT+CMGR Read Message

AT+CMGR read command returns SMS message with location value <index> from message storage <mem1> to the TE. If status of the message is “REC UNREAD”, status in the storage changes to “REC READ”.

AT+CMGR
Read Message

Test Command

```
AT+CMGR=?
```

Response

```
OK
```

Write Command

```
AT+CMGR=<index>
```

Response
TA returns SMS message with location value <index> from message storage <mem1> to the TE. If status of the message is “REC UNREAD”, status in the storage changes to “REC READ”.

If text mode (+CMGF=1) and command is executed successfully:

For SMS-DELIVER:

```
+CMGR:
<stat>,<oa>,[<alpha>],<scts>[,<tooa>,<fo>,<pid>,<dcs>,<sca>,<tosca>,<length>]<CR>
↪<LF><data>

OK
```

For SMS-SUBMIT:

```
+CMGR:
<stat>,<da>,[<alpha>][,<toda>,<fo>,<pid>,<dcs>,[<vp>],<sca>,<tosca>,<length>]<CR>
↪<LF><data>

OK
```

For SMS-STATUS-REPORTs:

```
+CMGR:
<stat>,<fo>,<mr>,[<ra>],[<tora>],<scts>,<dt>,<st>

OK
```

For SMS-COMMANDs:

```
+CMGR:

<stat>,<fo>,<ct>[,<pid>,[<mn>],[<da>],[<toda>],<length><CR><LF><cdata>]

OK
```

For CBM storage:

```
+CMGR:

<stat>,<sn>,<mid>,<dcs>,<page>,<pages><CR><LF><data>

OK
```

If PDU mode (+CMGF=0) and command successful:

```
+CMGR: <stat>,[<alpha>],<length><CR><LF><pdu>

OK
```

Maximum Response Time
Depends on the length of message content.

Reference
3GPP TS 27.005

Parameter

<index>
Integer type, in the range of location numbers supported by the associated memory

<stat>

Text mode explanation

"REC UNREAD"
Received unread messages

"REC READ"
Received read messages

"STO UNSENT"
Stored unsent messages

"STO SENT"
Stored sent messages

"ALL"
All messages

PDU mode explanation

0
Received unread messages

1
Received read messages

2
Stored unsent messages

3
Stored sent messages

4
All messages

<alpha>
String type alphanumeric representation of <da> or <oa> corresponding to the entry found in MT phonebook; implementation of this feature is manufacturer specified; the used character set should be the one selected with command Select TE Character Set AT+CSCS (see definition of this command in 3GPP TS 27.007).

<da>
Destination address. 3GPP TS 23.040 TP-Destination-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in 3GPP TS 27.007); type of address is given by <toda>.

<oa>
Originating address. 3GPP TS 23.040 TP-Originating-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command +CSCS in TS 27.007); type of address is given by <tooa>.

<scts>
Service center time stamp. 3GPP TS 23.040 TP-Service-Centre-Time-Stamp in time-string format (refer to <dt>).

<fo>
First octet. Depending on the command or result code: First octet of 3GPP TS 23.040 SMS-DELIVER, SMS-SUBMIT (default 17), SMS-STATUS-REPORT, or SMS-COMMAND in integer format. If a valid value has been entered once, parameter can be omitted.

<pid>
Protocol identifier. 3GPP TS 23.040 TP-Protocol-Identifier in integer format (default 0).

<dcs>
Data coding scheme. Depending on the command or result code: 3GPP TS 23.038 SMS Data Coding Scheme (default 0), or Cell Broadcast Data Coding Scheme in integer format.

<vp>
Validity period. Depending on SMS-SUBMIT <fo> setting: 3GPP TS 23.040 TP-Validity-Period either in integer format or in time-string format (refer to <dt>).

<mn>
Message number. 3GPP TS 23.040 TP-Message-Number in integer format.

<mr>
Message reference. 3GPP TS 23.040 TP-Message-Reference in integer format.

<ra>
Recipient address. 3GPP TS 23.040 TP-Recipient-Address Address-Value field in string format; BCD numbers (or GSM default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS.); type of address given by <tora>.

<tora>
Type of recipient address. 3GPP TS 24.011 TP-Recipient-Address Type-of-Address octet in integer format (default refer <toda>).

<toda>
Type of recipient address. 3GPP TS 24.011 TP-Recipient-Address Type-of-Address octet in integer format.

<tooa>
Type of originating address.3GPP TS 24.011 TP-Originating-Address Type-of-Address octet in integer format (default refer to <toda>).

<sca>
Service center address. 3GPP TS 24.011 RP SC address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command +CSCS in 3GPP TS 27.007); type of address is given by <tosca>.

<tosca>
Type of service center address. 3GPP TS 24.011 RP SC address Type-of-Address octet in integer format (default refer to <toda>).

<length>
Message length, integer type, indicating in the text mode (AT+CMGF=1) the length of the message body <data> (or <cdata>) in characters; or in PDU mode (AT+CMGF=0) the length of the actual TP data unit in octets (i.e. the RP layer SMSC address octets are not counted in the length).

<data>
The text of short message. Please refer 14.8 SMS Character Sets Conversions for the detail.

<pdu>
In the case of SMS: 3GPP TS 24.011 SC address followed by 3GPP TS 23.040 TPDU in hexadecimal format: ME/TA converts each octet of TP data unit into two IRA character long hexadecimal number (e.g. octet with integer value 42 is presented to TE as two characters 2A (IRA 50 and 65))3GPP TS 27.007.

<prt>

Priority

0
Normal

1
Interactive

2
Urgent

3
Emergency

<fmt>

Format

0
GSM 7 bit

1
ASCII

6
UNICODE

<prv>

Privacy

0
Normal

1
Restricted

2
Confidential

3
Secret

<lang>

Language

0
Unspecified

1
English

2
French

3
Spanish

4
Japanese

5
Korean

6
Chinese

7
Hebrew

<type>

0
Normal

1
CPT

2
Voice Mail

3
SMS Report

Example

```
+CMTI: “SM”,3   //Indicates that new message has been received and saved to
↪<index>=3 of “SM”
```

(continues on next page)

(continued from previous page)

```
AT+CSDH=1
OK
AT+CMGR=3       //Read message
+CMGR:  “REC  UNREAD”,“+8615021012496”,,“13/12/13,15:06:37+32”,145,4,0,0,
↪“+8613800210500”,145,27

<This is a test>

OK
```

AT+CMGS Send Message

AT+CMGS write command sends a short message from TE to network (SMS-SUBMIT). After invoking the write command, wait for the prompt “>” and then start to write the message. After that, enter <CTRL-Z> to indicate the ending of PDU and begin to send the message. Sending can be cancelled by giving <ESC> character. Abortion is acknowledged with “OK”, though the message will not be sent. The message reference <mr> is returned to the TE on successful message delivery. The value can be used to identify message upon unsolicited delivery status report result code.

AT+CMGS
Send Message

Test Command

```
AT+CMGS=?
```

Response

```
OK
```

Write Command

1. If text mode (AT+CMGF=1):

```
AT+CMGS=<da>[,<toda>]<CR>

text is entered

<ctrl-Z/ESC>

ESC quits without sending
```

2. If PDU mode (AT+CMGF=0):

```
AT+CMGS=<length><CR>

PDU is given <ctrl-Z/ESC>
```

Response
TA sends message from TE to the network (SMS-SUBMIT). Message reference value <mr> is returned to the TE on successful message delivery. Optionally (when AT+CSMS <service> value is 1 and network supports) <scts> is returned. Values can be used to identify message upon unsolicited delivery status report result code.

If text mode (AT+CMGF=1) and sent successfully:

```
+CMGS: <mr>

OK
```

If PDU mode (AT+CMGF=0) and sent successfully:

```
+CMGS: <mr>

OK
```

If error is related to ME functionality:

```
+CMS ERROR: <err>
```

Maximum Response Time
120s, determined by network.

Reference
3GPP TS 27.005

Parameter

<da>
Destination address. 3GPP TS 23.040 TP-Destination-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in 3GPP TS 27.007); type of address is given by <toda>.

<toda>
Type of recipient address. 3GPP TS 24.011 TP-Recipient-Address Type-of-Address octet in integer format.

<length>
Message length. Integer type, indicating in the text mode (+CMGF=1) the length of the message body <data> (or <cdata>) in characters; or in PDU mode (+CMGF=0), the length of the actual TP data unit in octets (i.e. the RP layer SMSC address octets are not counted in the length).

<mr>
Message reference. 3GPP TS 23.040 TP-Message-Reference in integer format.

Example

```
AT+CMGF=1           //Set SMS message format as text mode
OK
AT+CSCS="GSM"       //Set character set as GSM which is used by the TE
OK
AT+CMGS="15021012496"

> <This is a test>                    //Enter in text, <CTRL+Z> send message,
↪<ESC> quits
                                      //without sending
+CMGS: 247

OK
```

AT+CMGW Write Message to Memory

AT+CMGW write and execution commands store a short message from TE to memory storage <mem2>. Memory location <index> of the stored message is returned. Message status will be set to "stored unsent" by default; but parameter <stat> also allows other status values to be given.

The syntax of input text is the same as the one specified in the write command AT+CMGS.

AT+CMGW
Write Message to Memory

Test Command

```
AT+CMGW=?
```

Response

```
OK
```

Write Command

1. If text mode (AT+CMGF=1): AT+CMGW=<oa/da>[,<tooa/toda>[,<stat>]]<CR> text is entered <ctrl-Z/ESC> <ESC> quits without sending
2. If PDU mode (AT+CMGF=0): AT+CMGW=<length>[,<stat>]<CR> PDU is given <ctrl-Z/ESC>

Response

TA transmits SMS message (either SMS-DELIVER or SMS-SUBMIT) from TE to memory storage <mem2>. Memory location <index> of the stored message is returned. By default message status will be set to „stored unsent', but parameter <stat> also allows other status values to be given.

If writing is successful:

```
+CMGW: <index>

OK
```

If error is related to ME functionality:

```
+CMS ERROR: <err>
```

Maximum Response Time

300ms

Reference

3GPP TS 27.005

Parameter

<da>

Destination address. 3GPP TS 23.040 TP-Destination-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in 3GPP TS 27.007); type of address is given by <toda>.

<oa>

Originating address. 3GPP TS 23.040 TP-Originating-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in TS 27.007); type of address given by <tooa>.

<tooa>

Type of originating address. 3GPP TS 24.011 TP-Originating-Address Type-of-Address octet in integer format (default refer to <toda>).

<stat>

PDU mode	Text mode	Explanation
0	"REC UNREAD"	Received unread messages
1	"REC READ"	Received read messages
2	"STO UNSENT"	Stored unsent messages
3	"STO SENT"	Stored sent messages
4	"ALL"	All messages

<toda>
Type of recipient address. 3GPP TS 24.011 TP-Recipient-Address Type-of-Address octet in integer format.

<length>
Message length. Integer type, indicating in the text mode (AT+CMGF=1) the length of the message body <data> (or <cdata>) in characters; or in PDU mode (AT+CMGF=0), the length of the actual TP data unit in octets (i.e. the RP layer SMSC address octets are not counted in the length).

<pdu>
In the case of SMS: 3GPP TS 24.011 SC address followed by 3GPP TS 23.04TPDU in hexadecimal format: ME/TA converts each octet of TP data unit into two IRA character long hexadecimal number (e.g. octet with integer value 42 is presented to TE as two characters 2A (IRA 50 and 65)).

<index>
Index of message in selected storage <mem2>.

Note

The command in CDMA network now only supports Text mode.

Example

```
AT+CMGF=1       //Set SMS message format as text mode
OK
AT+CSCS="GSM"   //Set character set as GSM which is used by the TE
OK
AT+CMGW="15021012496"

> <This is a test>     //Enter in text, <CTRL+Z> write message, <ESC> quits␣
↪without sending

+CMGW: 4
OK
AT+CMGF=0                          //Set SMS message format as PDU mode
OK
AT+CMGW=18
> 0051FF00000008000A0500030002016D4B8BD5
+CMGW: 5

OK
```

AT+CMSS Send Message from Storage

AT+CMSS write command sends message with location value <index> from message storage <mem2> to the network. If new recipient address <da> is given for SMS-SUBMIT, it shall be used instead of the one stored with the message.

AT+CMSS
Send Message from Storage

Test Command

```
AT+CMSS=?
```

Response

```
OK
```

Write Command

```
AT+CMSS=<index>[,<da>[,<toda>]]
```

Response

TA sends message with location value <index> from message storage <mem2> to the network (SMS-SUBMIT). If new recipient address <da> is given, it shall be used instead of the one stored with the message. Reference value <mr> is returned to the TE on successful message delivery. Values can be used to identify message upon unsolicited delivery status report result code.

1. **If text mode (AT+CMGF=1) and sent successfully:**

```
+CMSS: <mr>[,<scts>]

OK
```

2. **If PDU mode (AT+CMGF=0) and sent successfully:**

```
+CMSS: <mr> [,<ackpdu>]

OK
```

3. **If error is related to ME functionality:**

```
+CMS ERROR: <err>
```

Maximum Response Time

120s, determined by network.

Reference

3GPP TS 27.005

Parameter

<index>

Integer type, in the range of location numbers supported by the associated memory.

<da>

Destination Address. 3GPP TS 23.040 TP-Destination-Address Address-Value field in string format; BCD numbers (or GSM 7 bit default alphabet characters) are converted to characters of the currently selected TE character set (refer to command AT+CSCS in 3GPP TS 27.007); type of address is given by <toda>.

<toda>

Type of recipient address. 3GPP TS 24.011 TP-Recipient-Address Type-of-Address octet in integer format.

<mr>

Message reference. 3GPP TS 23.040 TP-Message-Reference in integer format.

<scts>

Service center time stamp. 3GPP TS 23.040 TP-Service-Centre-Time-Stamp in time-string format (refer to <dt>).

<ackpdu>

Format is same for <pdu> in case of SMS, but without 3GPP TS 24.011 SC address field and parameter shall be bounded by double quote characters like a normal string type parameter.

Example

```
AT+CMGF=1                    //Set SMS message format as text mode
OK
AT+CSCS="GSM"                //Set character set as GSM which is used by the TE
OK
AT+CMGW="15021012496"
```

(continues on next page)

(continued from previous page)

```
> Hello                        //Enter in text, <CTRL+Z> send message, <ESC> quits␣
↪without sending

+CMGW: 4

OK
AT+CMSS=4                                                          //Send the␣
↪message of index 4 from memory storage.
+CMSS: 54

OK
```

AT+CNMI SMS Event Reporting Configuration

AT+CNMI write command selects the procedure on how the received new messages from the network are indicated to the TE when TE is active, e.g. DTR signal is ON. If TE is inactive (e.g. DTR signal is OFF), message receiving should be done as specified in 3GPP TS 23.038.

AT+CNMI
SMS Event Reporting Configuration

Test Command

```
AT+CNMI=?
```

Response

```
+CNMI: (list of supported <mode>s),(list of supported
<mt>s),(list of supported <bm>s),(list of supported
<ds>s),(list of supported <bfr>s)

OK
```

Read Command

```
AT+CNMI?
```

Response

```
+CNMI: <mode>,<mt>,<bm>,<ds>,<bfr>

OK
```

Write Command

```
AT+CNMI[=<mode>[,<mt>[,<bm>[,<ds>[,<bfr>]]]]]
```

Response
TA selects the procedure on how the received new messages from the network are indicated to the TE when TE is active, e.g. DTR signal is ON. If TE is inactive (e.g. DTR signal is OFF), message receiving should be done as specified in 3GPP TS 23.038.

```
OK

ERROR
```

If error is related to ME functionality:

```
+CMS ERROR: <err>
```

Maximum Response Time
300ms

Reference
3GPP TS 27.005

Parameter

<mode>

0
Buffer unsolicited result codes in the TA. If TA result code buffer is full, indications can be buffered in some other place or the oldest indications may be discarded and replaced with the new received indications.

1
Discard indication and reject new received message unsolicited result codes when TA-TE link is reserved (e.g. in on-line data mode). Otherwise forward them directly to the TE.

2
Buffer unsolicited result codes in the TA when TA-TE link is reserved (e.g. in on-line data mode) and flush them to the TE after reservation. Otherwise forward them directly to the TE.

<mt>
The rules for storing received SMS depend on its data coding scheme (refer to 3GPPTS 23.038) and preferred memory storage (+CPMS) setting; and the value is:

0
No SMS-DELIVER indications are routed to the TE.

1
If SMS-DELIVER is stored into ME/TA, indication of the memory location is routed to the TE by using unsolicited result code: +CMTI: <mem>,<index>

2
SMS-DELIVERs (except class 2) are routed directly to the TE using unsolicited result code:

PDU Mode

```
+CMT: [<alpha>],<length><CR><LF><pdu>
```

Text mode

```
+CMT:<oa>,[<alpha>],<scts>[,<tooa>,<fo>,<pid>,<dcs>,<sca>,<tosca>,
↪<length>]<CR><LF><data>
```

Text mode for CDMA SMS

```
^HCMT: <oa>,<scts>,<lang>,<fmt>,<length>,<prt>,<prv>,<type>,<stat><CR>
↪<LF><data>
```

Class 2 messages result in indication as defined in <mt>=1.

3
Class 3 SMS-DELIVERs are routed directly to TE by using unsolicited result codes defined in <mt>=2. Messages of other classes result in indication as defined in <mt>=1.

<bm>
The rules for storing received CBMs depend on its data coding scheme (refer to 3GPP TS 23.038) and the setting of Select CBM Types (+CSCB); and the value is:

0
No CBM indications are routed to the TE.

2

New CBMs are routed directly to the TE using unsolicited result code:

PDU mode

```
+CBM: <length><CR><LF><pdu>
```

Text mode

```
+CBM: <sn>,<mid>,<dcs>,<page>,<pages><CR><LF><data>
```

3

Class 3 CBMs are routed directly to TE by using unsolicited result codes defined in **<bm>** =2. If CBM storage is supported, messages of other classes result in indication as defined in **<bm>** =1.

<ds>

0

No SMS-STATUS-REPORTs are routed to the TE.

1

SMS-STATUS-REPORTs are routed to the TE using unsolicited result code:

PDU mode

```
+CDS: <length><CR><LF><pdu>
```

Text mode

```
+CDS: <fo>,<mr>,[<ra>],[<tora>],<scts>,,<st>
```

2

If SMS-STATUS-REPORT is stored into ME/TA, indication of the memory location is routed to the TE using unsolicited result code:

```
+CDSI:<mem>,<index>
```

<bfr>

0

TA buffer of unsolicited result codes defined within this command is flushed to the TE when <mode> 1...2 is entered ("OK" response shall be given before flushing the codes).

1

TA buffer of unsolicited result codes defined within this command is cleared when <mode> 1...2 is entered.

Note

Unsolicited result code:

+CMTI: <mem>,<index>
Indicates that new message has been received

+CMT: [<alpha>],<length><CR><LF><pdu>
Short message is outputted directly

+CBM: <length><CR><LF><pdu>
Cell broadcast message is outputted directly

Example

```
AT+CMGF=1            //Set SMS message format as text mode
OK
AT+CSCS="GSM"        //Set character set as GSM which is used by the TE
OK
AT+CNMI=1,2,0,1,0    //Set SMS-DELIVERs are routed directly to the TE
OK

+CMT: "+8615021012496",,"13/03/18,17:07:21+32",145,4,0,0,"+8613800551500",145,28

This is a test.         //Short message is outputted directly when SMS is␣
↪incoming.
```

AT+CSDH Show SMS Text Mode Parameters

AT+CSDH write command controls whether detailed header information is shown in text mode result codes.

AT+CSDH
Show SMS Text Mode Parameters

Test Command

```
AT+CSDH=?
```

Response

```
+CSDH: (list of supported <show>s)

OK
```

Read Command

```
AT+CSDH?
```

Response

```
+CSDH: <show>

OK
```

Write Command

```
AT+CSDH[=<show>]
```

Response

```
OK
ERROR
```

Maximum Response Time
300ms

Reference
3GPP TS 27.005

Parameter

<show>

0
Do not show header values defined in commands +CSCA, +CSMP (<sca>, <tosca>, <fo>, <vp>, <pid>, <dcs>) and <length>, <toda> or <tooa> in +CMT, +CMGL, +CMGR result codes for SMS-DELIVERs and SMS-SUBMITs in text mode

1
Show the values in result codes

Example

```
AT+CSDH=0
OK
AT+CMGR=2
+CMGR: “STO UNSENT” ,“”,

<This is a test>

OK
AT+CSDH=1
OK
AT+CMGR=2
+CMGR: “STO UNSENT”,“”,,128,17,0,0,143,“+8613800551500”,145,18

<This is a test>

OK
```

AT+CSMP Set SMS Text Mode Parameters

AT+CSMP is used to set values for additional parameters needed when a short message is sent to the network or placed in a storage in text mode.

AT+CSMP
Set SMS Text Mode Parameters

Test Command

```
AT+CSMP=?
```

Response

```
OK
```

Read Command

```
AT+CSMP?
```

Response

```
+CSMP: <fo>,<vp>,<pid>,<dcs>

OK
```

Write Command

```
AT+CSMP=<fo>[,<vp>[,<pid>[,<dcs>]]]
```

Response
TA selects values for additional parameters needed when SM is sent to the network or placed in a storage when text mode is selected (AT+CMGF=1). It is possible to set the validity period starting from when the SM is received by the SMSC (<vp> ranges from 0 to 255) or define the absolute time of the validity period termination (<vp> is a string).

```
OK
```

Maximum Response Time
300ms

Reference
3GPP TS 27.005

Parameter

<fo>
First octet. Depending on the command or result code: First octet of 3GPP TS 23.040 SMS-DELIVER, SMS-SUBMIT (default 17), SMS-STATUS-REPORT, SMS-COMMAND in integer format. If a valid value has been entered once, parameter can be omitted.

<vp>
Validity period. Depending on SMS-SUBMIT <fo> setting: 3GPP TS 23.040 TP-Validity-Period either in integer format or in time-string format (refer to <dt>).

<pid>
Protocol identifier. 3GPP TS 23.040 TP-Protocol-Identifier in integer format (default 0).

<dcs>
Data coding scheme. Depending on the command or result code: 3GPP TS 23.038 SMS Data Coding Scheme (default 0), or Cell Broadcast Data Coding Scheme in integer format.

A.1.8 Commands for packet domain

AT+CGDCONT Define PDP Context

AT+CGDCONT specifies PDP context parameters for a specific context <cid>. A special form of the write command (AT+CGDCONT=<cid>) causes the values for context <cid> to become undefined. It is not allowed to change the definition of an already activated context.

The AT+CGDCONT read command returns the current settings for each defined PDP context.

AT+CGDCONT
Define PDP Context

Test Command

```
AT+CGDCONT=?
```

Response

```
+CGDCONT: (range of supported <cid>s), <PDP_type>,
<APN>, <PDP_addr>, (list of supported <data_comp>s),
(list of supported <head_comp>s)

OK
```

Read Command

```
AT+CGDCONT?
```

Response

```
+CGDCONT:
<cid>,<PDP_type>,<APN>,<PDP_addr>,<data_comp>,<head_comp>[...]

OK
```

Write Command

```
AT+CGDCONT=<cid>[,<PDP_type>[,<APN>[,<PDP_addr>[,<data_comp>[,<head_comp>]]]]]
```

Response

```
OK
ERROR
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<cid>
PDP context identifier, a numeric parameter which specifies a particular PDP context definition. The parameter is local to the TE-MT interface and is used in other PDP context-related commands. The range of permitted values (minimum value=1) is returned by the test form of the command.

<PDP_type>
Packet data protocol type, a string parameter which specifies the type of packet data protocol.

- "IP" IPV4
- "PPP"
- "IPV6"
- "IPV4V6"

<APN>
Access point name, a string parameter that is a logical name used to select the GGSN or the external packet data network. If the value is null or omitted, then the subscription value will be requested.

<PDP_addr>
A string parameter identifies the MT in the address space applicable to the PDP. If the value is null or omitted, then a value may be provided by the TE during the PDP startup procedure or, failing that, a dynamic address will be requested. The allocated address may be read using the AT+CGPADDR command.

<data_comp>
A numeric parameter that controls PDP data compression (applicable for SNDCP only) (refer to 3GPP TS 44.065).

0
Off (Default if value is omitted)

1
On (Manufacturer preferred compression)

2
V.42bis

3
V.44 (Not supported currently)

<head_comp>
A numeric parameter that controls PDP header compression (refer to 3GPP TS 44.065 and 3GPP TS 25.323).

0
Off

1
On

2
RFC1144

3
RFC2507

4
RFC3095

AT+CGREG Network Registration Status

The AT+CGREG command queries the network registration status and controls the presentation of an unsolicited result code +CGREG: <stat> when <n>=1 and there is a change in the MT's GPRS network registration status in GERAN/UTRAN, or unsolicited result code +CGREG: <stat>[,[<lac>],[<ci>],[<Act>],[<rac>]] when <n>=2 and there is a change of the network cell in GERAN/UTRAN.

AT+CGREG
Network Registration Status

Test Command

```
AT+CGREG=?
```

Response

```
+CGREG: (list of supported <n>s)

OK
```

Read Command

```
AT+CGREG?
```

Response
In Non-CDMA mode:

```
+CGREG: <n>,<stat>[,<lac>,<ci>[,<Act>]]

OK
```

In CDMA mode:

```
+CGREG: <n>,<stat>[,<sid>,<nid_bid>,<Act>]

OK
```

Write Command

```
AT+CGREG[=<n>]
```

Response

```
OK
ERROR
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<n>

0
Disable network registration unsolicited result code

1

Enable network registration unsolicited result code +CGREG:<stat>

2

Enable network registration and location information unsolicited result code +CGREG: <stat>[,<lac>,<ci>[,<Act>]]

<stat>

0

Not registered, MT is not currently searching an operator to register to .The UE is in GMM state GMM-NULL or GMM-DEREGISTERED-INITIATED. The GPRS service is disabled; the UE is allowed to attach for GPRS if requested by the user.

1

Registered, home network .The UE is in GMM state GMM-REGISTERED or GMM-ROUTING-AREA-UPDATING-INITIATED INITIATED on the home PLMN.

2

Not registered, but MT is currently trying to attach or searching an operator to register to. The UE is in GMM state GMM-DEREGISTERED or GMM-REGISTERED-INITIATED. The GPRS service is enabled, but an allowable PLMN is currently not available. The UE will start a GPRS attach as soon as an allowable PLMN is available.

3

Registration denied. The UE is in GMM state GMM-NULL. The GPRS service is disabled; and the UE is not allowed to attach for GPRS if requested by the user.

4

Unknown

5

Registered, roaming

<lac>

String type, two bytes location area code in hexadecimal format (e.g. “00C3” equals 195 in decimal)

<ci>

String type, two byte cell ID in hexadecimal format

<Act>

Access technology selected

0

GSM

2

UTRAN

3

GSM W/EGPRS

4

UTRAN W/HSDPA

5

UTRAN W/HSUPA

6

UTRAN W/HSDPA and HSUPA

7

E-UTRAN

Example

```
AT+CGREG?
+CGREG: 0,1

OK
```

A.1.9 Hardware Related Commands

AT+CCLK Clock

AT+CCLK sets and queries the real time clock (RTC) of the module. The current setting is retained until the module is totally disconnected from power.

AT+CCLK
Clock

Test Command

```
AT+CCLK=?
```

Response

```
OK
```

Read Command

```
AT+CCLK?
```

Response

```
+CCLK: <time>

OK
```

Write Command

```
AT+CCLK=<time>
```

Response

```
OK
```

If error is related to ME functionality:

```
+CME ERROR: <err>
```

Maximum Response Time
300ms

Reference
3GPP TS 27.007

Parameter

<time>
String type value, format is "yy/MM/dd,hh:mm:ss±zz", indicating year (two last digits), month, day, hour, minutes, seconds and time zone (indicates the difference, expressed in quarters of an hour, between the local time and GMT; range -48…+56). E.g. May 6th, 1994, 22:10:00 GMT+2 hours equals to "94/05/06,22:10:00+08".

Example

```
AT+CCLK?
+CCLK: “08/01/04,00:19:43+00”

OK
```

https://www.cybertec.com.au